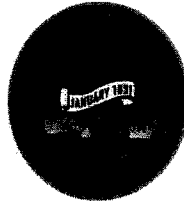


1550-14939

PROFESSIONAL SERVICES AGREEMENT

MANAGED SECURITY SERVICE PROVIDER

BETWEEN



COOK COUNTY GOVERNMENT

THE DEPARTMENT OF HOMELAND SECURITY AND EMERGENCY MANAGEMENT

AND

SECUREWORKS, INC.

CONTRACT NO. 1550-14939

APPROVED BY THE BOARD OF
COOK COUNTY COMMISSIONERS

JUN 13 2016

PROFESSIONAL SERVICES AGREEMENT

TABLE OF CONTENTS

TERMS AND CONDITIONS	3
ARTICLE 1) INCORPORATION OF BACKGROUND	3
ARTICLE 2) DEFINITIONS.....	3
a) Definitions.....	3
b) Interpretation.....	4
c) Incorporation of Exhibits	4
ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT.....	5
a) Scope of Services.....	5
b) Deliverables.....	5
c) Standard of Performance.....	6
d) Personnel.....	6
e) Minority and Women Owned Business Enterprises Commitment.....	7
f) Insurance.....	7
g) Indemnification	9
h) Confidentiality and Ownership of Documents	10
i) Intellectual Property Rights	11
j) Customer License to Customization	11
k) Examination of Records and Audits	12
l) Subcontracting or Assignment of Contract or Contract Funds.....	13
m) Limitation of Liability.....	14
ARTICLE 4) TERM OF PERFORMANCE.....	15
a) Term of Performance	15
b) Timeliness of Performance	15
c) Agreement Extension Option.....	15
ARTICLE 5) COMPENSATION	15
a) Basis of Payment.....	15
b) Method of Payment.....	16
c) Funding.....	16
d) Non-Appropriation.....	16
e) Taxes.....	17
f) Nonpayment.....	17
ARTICLE 6) DISPUTES.....	17
ARTICLE 7) COOPERATION WITH INSPECTOR GENERAL AND COMPLIANCE WITH ALL LAWS.....	18
ARTICLE 8) SPECIAL CONDITIONS.....	18
a) Warranties and Representations.....	18
b) Ethics.....	19
c) Business Documents	19
d) Conflicts of Interest.....	19
e) Non-Liability of Public Officials	20
ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION AND RIGHT TO OFFSET.....	20
a) Events of Default Defined	20
b) Remedies	21
c) Early Termination	22

d)	Suspension.....	23
e)	Right to Offset.....	23
f)	Delays.....	24
g)	Prepaid Fees.....	24
ARTICLE 10) GENERAL CONDITIONS		24
a)	Entire Agreement.....	24
b)	Counterparts.....	25
c)	Contract Amendments	25
d)	Governing Law and Jurisdiction.....	25
e)	Severability.....	25
f)	Assigns.....	26
g)	Cooperation.....	26
h)	Waiver.....	26
i)	Independent Consultant	27
j)	Governmental Joint Purchasing Agreement	27
ARTICLE 11) NOTICES.....		28
ARTICLE 12) AUTHORITY		28

List of Exhibits

Exhibit 1	Scope of Services
Exhibit 2	Schedule of Compensation
Exhibit 3	Minority and Women Owned Business Enterprise Commitment and MBE/WBE Utilization Plan
Exhibit 4	Evidence of Insurance
Exhibit 5	Board Authorization
Exhibit 6	Identification of Subcontractor/Supplier/Subconsultant Form
Exhibit 7	Cook County Travel and Transportation Policy
Exhibit 8	IT Special Conditions
Exhibit 9	Dell SecureWorks Software License and Services Agreement
Exhibit 10	Grant Agreement
Exhibit 11	Federal Clause
Exhibit 12	Economic Disclosure Statement
	Signature Page

AGREEMENT

This Professional Services Agreement for Managed Security Services (the "Agreement") is made and entered into by and between the County of Cook, a public body corporate of the **STATE OF ILLINOIS**, on behalf of Office of the Chief Procurement Officer hereinafter referred to as "**County**" or the "**Customer**" and **SECUREWORKS, INC.**, doing business as a(an) Corporation of the State of Georgia hereinafter referred to as "**Consultant**" or "**SecureWorks**", pursuant to authorization by the Cook County Board of Commissioners on July 13, 2016, as evidenced by Board Authorization letter attached hereto as EXHIBIT "5".

BACKGROUND

The County of Cook issued a Request for Proposals "RFP" for Managed Security Service Provider. Proposals were evaluated in accordance with the evaluation criteria published in the RFP. The Consultant was selected based on the proposal submitted and evaluated by the County representatives.

Consultant represents that it has the professional experience and expertise to provide the necessary services and further warrants that it is ready, willing and able to perform in accordance with the terms and conditions as set forth in this Agreement.

NOW, THEREFORE, the County and Consultant agree as follows:

TERMS AND CONDITIONS

ARTICLE 1) INCORPORATION OF BACKGROUND

The Background information set forth above is incorporated by reference as if fully set forth here.

ARTICLE 2) DEFINITIONS

a) Definitions

The following words and phrases have the following meanings for purposes of this Agreement:

"Additional Services" means those services which are within the general scope of Services of this Agreement, but beyond the description of services required under Article 3, and all services reasonably necessary to complete the Additional Services to the standards of performance required by this Agreement. Any Additional Services requested by the Using Agency require the approval of the Chief Procurement Officer in a written amendment to this Agreement before Consultant is obligated to perform those Additional Services and before the County becomes obligated to pay for those Additional Services.

"Agreement" means this Professional Services Agreement, including all exhibits attached to it and incorporated in it by reference, and all amendments, modifications or revisions made in accordance with its terms.

"Chief Procurement Officer" means the Chief Procurement Officer for the County of Cook and any representative duly authorized in writing to act on his behalf.

"**Services**" means, collectively, the services, duties and responsibilities described in Article 3 of this Agreement and any and all work necessary to complete them or carry them out fully and to the standard of performance required in this Agreement.

"**Subcontractor**" or "**Subconsultant**" means any person or entity with whom Consultant contracts to provide any part of the Services on Consultant's behalf.

"**Using Agency**" shall mean the department of agency within Cook County including elected officials.

b) Interpretation

- i) The term "**include**" (in all its forms) means "include, without limitation" unless the context clearly states otherwise.
- ii) All references in this Agreement to Articles, Sections or Exhibits, unless otherwise expressed or indicated are to the Articles, Sections or Exhibits of this Agreement.
- iii) Words importing persons include firms, associations, partnerships, trusts, corporations and other legal entities, including public bodies, as well as natural persons.
- iv) Any headings preceding the text of the Articles and Sections of this Agreement, and any tables of contents or marginal notes appended to it are solely for convenience or reference and do not constitute a part of this Agreement, nor do they affect the meaning, construction or effect of this Agreement.
- v) Words importing the singular include the plural and vice versa. Words of the masculine gender include the correlative words of the feminine and neuter genders.
- vi) All references to a number of days mean calendar days, unless expressly indicated otherwise.

c) Incorporation of Exhibits

The following attached Exhibits are made a part of this Agreement:

Exhibit 1	Scope of Services
Exhibit 2	Schedule of Compensation
Exhibit 3	Minority and Women Owned Business Enterprise Commitment and MBE/WBE Utilization Plan
Exhibit 4	Evidence of Insurance
Exhibit 5	Board Authorization
Exhibit 6	Identification of Subcontractor/Supplier/Subconsultant Form
Exhibit 7	Cook County Travel and Transportation Policy
Exhibit 8	IT Special Conditions
Exhibit 9	Dell SecureWorks Software License and Services Agreement
Exhibit 10	Grant Agreement

Exhibit 11 Federal Clause
Exhibit 12 Economic Disclosure Statement
 Signature Page

ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT

a) **Scope of Services**

During the term of this Agreement and subject to the terms and conditions herein, SecureWorks agrees to provide certain: (i) managed security services ("MSS Services"), and/or (ii) security risk consulting services ("Consulting Services") purchased by Customer. The MSS Services and Consulting Services are collectively referred to hereafter as the "Services". The Services that Consultant must provide include, but are not limited to, those described in Exhibit 1, Scope of Services and Time Limits for Performance, which is attached to this Agreement and incorporated by reference as if fully set forth here. Consultant must provide the Services in accordance with the standards of performance set forth in any SOWs/Service Orders and this Agreement.

The Services being purchased shall be specified in one or more service order(s) ("Service Order(s)") or statement(s) of work ("SOW(s)") executed by the parties. The Chief Information Security Officer shall execute service orders for the County and Consultant's authorized agent shall execute on its behalf. A detailed description of the MSS Services being purchased is provided in the service description and service level agreement ("SLA") for such MSS Services attached to each Service Order and incorporated therein by reference. All signed Services Orders and SOWs are subject to the terms and conditions of this Agreement and will include the following: (i) the particular Services to be performed, including, if applicable, any SLAs; (ii) the term of the Services; (iii) compensation and billing methods for the Services, as outlined in Exhibit 2; and (iv) any other applicable information agreed to by the parties. The term of any service order shall not exceed the term of this Agreement.

SecureWorks will provide the equipment or hardware as necessary for Customer to receive the MSS Services ("Equipment"). Upon the earlier of the termination or expiration of this Agreement and/or the applicable Service Order, Customer will return all Equipment to SecureWorks. If such Equipment is not returned by Customer, Customer will be responsible for the then-current replacement costs of such Equipment.

b) **Deliverables**

In carrying out Consulting Services, Consultant must prepare or provide to the County various Deliverables. "**Deliverables**" include written reviews, recommendations, reports and analyses, produced by Consultant specifically for the County.

Except as otherwise provided in an applicable SOW, the County may reject Deliverables that do not include relevant information or data, or do not include all documents or other materials specified in this Agreement or reasonably necessary for the purpose for which the County made this Agreement or for which the County intends to use the Deliverables. If the County determines that Consultant has failed to comply with the foregoing standards, it has thirty (30) calendar days from the delivery of the Deliverable to notify Consultant of its failure. If Consultant does not correct the failure, if it is possible to do so, within thirty (30) calendar days

after receipt of notice from the County specifying the failure, then the County, by written notice, may treat the failure as a default of this Agreement under Article 9.

Partial or incomplete Deliverables may be accepted for review only when required for a specific and well-defined purpose and when consented to in advance by the County. Such Deliverables will not be considered as satisfying the requirements of this Agreement and partial or incomplete Deliverables in no way relieve Consultant of its commitments under this Agreement.

c) Standard of Performance

Consultant must perform all Services required of it under this Agreement with that degree of skill, care and diligence normally shown by a consultant performing services of a scope and purpose and magnitude comparable with the nature of the Services to be provided under this Agreement. Consultant acknowledges that it is entrusted with or has access to valuable and confidential information and records of the County and with respect to that information, Consultant agrees to be held to the standard of care of a fiduciary.

Consultant must assure that all Services that require the exercise of professional skills or judgment are accomplished by professionals qualified and competent in the applicable discipline and appropriately licensed, if required by law. Consultant remains responsible for the professional and technical accuracy of all Services or Deliverables furnished, whether by Consultant or its Subconsultants or others on its behalf. All Deliverables must be prepared in a form and content satisfactory to the Using Agency and delivered in a timely manner consistent with the requirements of this Agreement.

If Consultant fails to comply with the foregoing standards, Consultant must perform again, at its own expense, all Services required to be re-performed as a direct or indirect result of that failure. Any review, approval, acceptance or payment for any of the Services by the County does not relieve Consultant of its responsibility for the professional skill and care and technical accuracy of its Services and Deliverables. This provision in no way limits the County's rights against Consultant either under this Agreement, at law or in equity.

d) Personnel

i) Adequate Staffing

During the term of any SOW and/or Service Order, and any extension thereof, Consultant must assign and maintain an adequate staff of competent personnel that is fully equipped, licensed as appropriate, available as needed, qualified and assigned to perform the Services. In the event that any personnel is specifically identified as a key person in a SOW (each a "Key Personnel"), SecureWorks will use commercially reasonable efforts not to replace such Key Personnel unless Customer so agrees, which agreement shall not be unreasonably withheld or delayed, except in the event the applicable Key Personnel resigns, is disabled or his/her employment is terminated by SecureWorks. If a Key Personnel is to be replaced whether at SecureWorks or Customer's reasonable and lawful request, SecureWorks will ensure a smooth transition of such Key Personnel. The replacement consultant provided by SecureWorks will become a Key Personnel and shall have substantially similar skills and experience as the Key Personnel being replaced.

e) **Minority and Women Owned Business Enterprises Commitment**

In the performance of this Agreement, including the procurement and lease of materials or equipment, Consultant must abide by the minority and women's business enterprise commitment requirements of the Cook County Ordinance, (Article IV, Section 34-267 through 272) except to the extent waived by the Compliance Director, which are set forth in Exhibit 3. Consultant's completed MBE/WBE Utilization Plan evidencing its compliance with this requirement are a part of this Agreement, in Form 1 of the MBE/WBE Utilization Plan, upon acceptance by the Compliance Director. Except to the extent waived by the Compliance Director, Consultant must utilize minority and women's business enterprises at the greater of the amounts committed to by the Consultant for this Agreement in accordance with Form 1 of the MBE/WBE Utilization Plan.

f) **Insurance**

Consultant must provide and maintain at Consultant's own expense, during the term of this Agreement and any time period following expiration if Consultant is required to return and perform any of the Services or Additional Services under this Agreement, the insurance coverages and requirements specified below, insuring Consultant's Services provided pursuant to this Agreement.

i) **Insurance To Be Provided**

(1) Workers Compensation and Employers Liability

Workers Compensation Insurance, as prescribed by applicable law, covering all employees who are to provide a service under this Agreement and Employers Liability coverage with limits of not less than \$500,000 each accident or illness.

(2) Commercial General Liability (Primary and Umbrella)

Commercial General Liability Insurance or equivalent with limits of not less than \$2,000,000 per occurrence for bodily injury, personal injury and property damage liability. Coverages must include the following: All premises and operations, products/completed operations, separation of insureds, defense and contractual liability. Cook County is to be named as an additional insured on a primary, non-contributory basis for liability arising directly or indirectly from the Services as respects insurable liabilities assumed by Consultant under this Agreement.

Subconsultants performing Services under this Agreement must maintain limits of not less than \$1,000,000 with the same terms in this Article 3(f).i(2).

(3) Automobile Liability (Primary and Umbrella)

When any motor vehicles (owned, non-owned and hired) are used in connection with Services to be performed, Consultant must provide Automobile Liability Insurance with limits of not less than \$1,000,000 per occurrence limit, for bodily injury and property damage. The County is to be named as an additional insured on a primary, non-contributory basis.

(4) Professional Liability

When any professional consultants perform Services in connection with this Agreement, Professional Liability Insurance covering acts, errors or omissions must be maintained with limits of not less than \$2,000,000. Coverage must include insurable contractual liability. When policies are renewed or replaced, the policy retroactive date must coincide with, or precede, start of Services on this Agreement. A claims-made policy which is not renewed or replaced must have an extended reporting period of two (2) years.

Subconsultants performing Services under this Agreement must maintain limits of not less than \$1,000,000 with the same terms in Article 3(f)i(4).

ii) **Additional Requirements**

- (1) Consultant must furnish the County of Cook, Cook County, Office of the Chief Procurement Officer, 118 N, Clark St., Room 1018, Chicago, IL 60602, certificates of insurance, or such similar evidence, to be in force on the date of this Agreement, and upon written request, Consultant will provide renewal certificates of insurance, or such similar evidence, if the coverages have an expiration or renewal date occurring during the term of this Agreement. Consultant must submit evidence of insurance prior to the effective date of the Agreement. The receipt of any certificate does not constitute agreement by the County that the insurance requirements in this Agreement have been fully met or that the insurance policies indicated on the certificate are in compliance with all Agreement requirements. The failure of the County to obtain certificates or other insurance evidence from Consultant is not a waiver by the County of any requirements for Consultant to obtain and maintain the specified coverages. Non-conforming insurance does not relieve Consultant of the obligation to provide insurance as specified in this Agreement. Nonfulfillment of the insurance conditions may constitute a violation of this Agreement, and the County retains the right to terminate this Agreement or to suspend this Agreement until proper evidence of insurance is provided.
- (2) All deductibles or self-insured retentions on referenced insurance coverages must be borne by Consultant. Consultant agrees that insurers waive their rights of subrogation against the County of Cook, its employees, elected officials, agents or representatives.
- (3) The coverages and limits furnished by Consultant in no way limit Consultant's liabilities and responsibilities specified within this Agreement or by law. Any insurance or self-insurance programs maintained by the County of Cook apply in excess of and do not contribute with insurance provided by Consultant under this Agreement.
- (4) The required insurance is not limited by any limitations expressed in the indemnification language in this Agreement or any limitation placed on the indemnity in this Agreement given as a matter of law.

- (5) Consultant must require all Subconsultants to provide the insurance required in this Agreement, or Consultant may provide the coverages for Subconsultants. All Subconsultants are subject to the same insurance requirements as Consultant unless otherwise specified in this Agreement. If Consultant or Subconsultant desires additional coverages, the party desiring the additional coverages is responsible for its acquisition and cost.
- (6) The County's Risk Management Office maintains the rights to modify, delete, alter or change these requirements based on the County's determination of changes in risk exposures. "**Risk Management Office**" means the Risk Management Office, which is under the direction of the Director of Risk Management and is charged with reviewing and analyzing insurance and related liability matters for the County.

g) Indemnification

SecureWorks shall defend, indemnify and hold harmless the Customer Indemnified Parties from any damages, costs and liabilities, expenses (including reasonable and actual attorney's fees) ("Damages") actually incurred or finally adjudicated as to any third-party claim or action alleging that the Products, MSS Services, Consulting Services or any Customer Reports prepared or produced by SecureWorks and delivered pursuant to this Agreement infringe or misappropriate any third party's patent, copyright, trade secret, or other intellectual property rights enforceable in the country(ies) in which the Products, MSS Services or any Customer Reports are performed or prepared for Customer by SecureWorks ("Indemnified Claims"). If an Indemnified Claim under this Section occurs, or if SecureWorks determines that an Indemnified Claim is likely to occur, SecureWorks shall, at its option: (A) obtain a right for Customer to continue using such Products, MSS Services or Customer Reports; (B) modify such Products, MSS Services or Customer Reports to make them non-infringing; or (C) replace such Products, MSS Services or Customer Reports with a non-infringing equivalent. If (A), (B) or (C) above are not reasonably available, either party may, at its option, terminate this MSSA and/or the relevant Service Order and SecureWorks will refund any pre-paid fees on a pro-rata basis for the allegedly infringing Products, MSS Services or Customer Reports that have not been performed or provided. Notwithstanding the foregoing, SecureWorks shall have no obligation under this Section for any claim resulting or arising from: (A) modifications made to the Products, MSS Services or Customer Reports that were not performed or provided by or on behalf of SecureWorks; or (B) the combination, operation or use by Customer or anyone acting on Customer's behalf, of the Products, MSS Services or Customer Reports in connection with a third-party product or service (the combination of which causes the infringement).

The Consultant covenants and agrees to indemnify and save harmless the County and its commissioners, officials, employees, agents and representatives, and their respective heirs, successors and assigns, from and against any and all costs, expenses, attorney's fees, losses, damages and liabilities incurred or suffered directly or indirectly from or attributable to any claims arising out the negligent performance or nonperformance of this Agreement by the Consultant, or the negligent acts or omissions of the officers, agents, employees, Consultants, subconsultants, licensees or invitees of the Consultant.

The Consultant agrees to indemnify and hold harmless the County from any third-party claim or

action, including those filed by County employees, (i) for personal bodily injuries, including death, or tangible property damage resulting from the Consultant's negligence or willful misconduct, and (ii) relating to Security violation or alleged violation of applicable export laws, regulations and orders.

County agrees to and does hereby assume sole responsibility for its own acts and omissions with respect to third parties which give rise to any claim arising out of this Agreement; provided, however, that Customer's responsibility or liability for any damages arising out of its acts and omissions are expressly subject to the limitations set forth in the Illinois Tort Immunity Act.

The Consultant expressly understands and agrees that any Performance Bond or insurance protection required of the Consultant, or otherwise provided by the Consultant, shall in no way limit the responsibility to indemnify the County as hereinabove provided.

h) Confidentiality and Ownership of Documents

Consultant acknowledges and agrees that information regarding this Agreement is confidential and shall not be disclosed, directly, indirectly or by implication, or be used by Consultant in any way, whether during the term of this Agreement or at any time thereafter, except solely as required in the course of Consultant's performance hereunder. Consultant shall comply with the applicable privacy laws and regulations affecting County and will not disclose any of County's records, materials, or other data to any third party. Consultant shall have the right to compile and distribute statistical analyses and reports utilizing data derived from information or data obtained from County; provided that such information or data shall be aggregated and Consultant may not use any such information or data that is identifiable to County without the prior written approval of County. In the event such approval is given, any such reports published and distributed by Consultant shall be furnished to County without charge.

SecureWorks will provide Customer with: (i) user IDs, tokens, passwords, (ii) access and use of the software (in object code format only), (iii) digital signatures, and (iv) access and use of the SecureWorks customer portal (the "Portal"), as necessary for Customer to receive the MSS Services (the "Software") and the applicable written directions and/or policies relating to the MSS Services, which may be in paper or electronic format (the "Documentation" and collectively, with the MSS Services, Equipment and the Software, the "Products"), or a combination thereof, as necessary for Customer to receive the MSS Services and access the Portal. SecureWorks grants to Customer a limited, nontransferable, royalty-free and nonexclusive license to access and use, and for Customer's Affiliate(s) to access and use, during the term of the MSS Services only, the Products delivered to Customer, subject to the restrictions set forth below.

Customer (i) will use the Products for its internal security purposes, or for the internal security purposes of Customer's Affiliates purchasing MSS Services hereunder, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) sell, rent, license, assign, distribute, or transfer any of the Products for commercial purposes; (b) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the Software; (c) copy any Software or Documentation, except that Customer may make a reasonable number of copies of the Documentation for its internal use (provided Customer reproduces on such copies all proprietary notices of SecureWorks or its suppliers); or (d) remove from any Software, Documentation or Equipment any language or designation indicating the confidential nature thereof or the proprietary rights of SecureWorks or its suppliers. In addition, Customer will not, and will not permit

unaffiliated third parties to, (I) use the Products on a time-sharing, outsourcing, service bureau, hosting, application service provider or managed service provider basis; (II) alter any aspect of any Software or Equipment; or (III) except as permitted under this Agreement, assign, transfer, distribute, or otherwise provide access to any of the Products to any unaffiliated third party or otherwise use any Product with or for the benefit of any unaffiliated third party.

Customer shall own all right, title and interest in and to any written summaries, reports, run books, analyses, and findings or other information or documentation prepared uniquely and exclusively for Customer in connection with the Services and as specified in a Service Order/SOW (the "Customer Reports"). The provision by Customer of any Customer Report or any information therein to any unaffiliated third party shall not entitle such unaffiliated third party to rely on the Customer Report or the contents thereof in any manner or for any purpose whatsoever, and SecureWorks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) to such unaffiliated third party arising from or related to reliance by such unaffiliated third party on any Customer Report or any contents thereof.

i) Intellectual Property Rights

SecureWorks' Proprietary Rights. As between Customer and SecureWorks, SecureWorks will own all right, title and interest in and to the Products and Services, other than those rights granted to the County under this Article 3(i). This Agreement does not transfer or convey to Customer or any third party, any right, title or interest in or to the Products and Services or any associated IP rights, other than those granted in the Customer Reports. SecureWorks agrees to transfer to Customer, all right, title and interest in and to any Customer Purchased Equipment, excluding any right, title or interest in and to the Software and any other SecureWorks IP loaded onto such Customer Purchased Equipment. In addition, Customer agrees that SecureWorks is the owner of all right, title and interest in all IP in any work, including, but not limited to, all inventions, methods, processes, and computer programs including any source code or object code, (and any enhancements and modifications made thereto) contained within the Services and/or Products (collectively, the "Works"), developed by SecureWorks in connection with the performance of the Services hereunder and of general applicability across SecureWorks' customer base, and Customer hereby assigns to SecureWorks all right, title and interest in and to any copyrights that Customer may have in and to such Work; provided, however, that such Work shall not include Customer's Confidential Information (as defined in Section 8), Customer Data, Customer Reports or other information belonging, referencing, identifying or pertaining to Customer or Customer Affiliates. Without limiting the foregoing, SecureWorks will own all right, title and interest in all IP in any advisory data, threat data, vulnerability data, analyses, summaries, bulletins and information made available to Customer in SecureWorks' provision of its Counter Threat Intelligence Services (the "TI Reports"), provided that SecureWorks grants to Customer a fully-paid, perpetual, irrevocable, non-exclusive, limited license to use, reproduce, modify, publicly display and create derivative works based upon all such TI Reports for use by Customer and its Affiliates.

j) Customer License to Customization

During the term of the Services, SecureWorks grants to Customer a limited, non-exclusive license to use such Works and TI Reports solely for Customer to receive the Services and for Customer's or its Affiliate's internal security purposes only. Customer acknowledges that any license to the SecureWorks Products, Services, Works and TI Reports, via customer portal, expires upon the expiration or termination of any individual Service Order/SOW and/or this Agreement.

Customer's Proprietary Rights. Customer represents and warrants that it has the necessary rights, power and authority to transmit Customer Data (as defined below) to SecureWorks under this Agreement. As between Customer and SecureWorks, Customer will own all right, title and interest in and to (i) any data provided by Customer and/or its Affiliate(s) to SecureWorks and/or Customer and/or its Affiliate(s)' data accessed or used by SecureWorks or transmitted by Customer and/or its Affiliate(s) to SecureWorks or SecureWorks Equipment in connection with SecureWorks' provision of the Services, including, but not limited to, Customer's and/or its Affiliate(s)' data included in any written or printed summaries, run books, analyses or reports generated in connection with the Services (Customer and its Affiliate(s)' data, collectively, the "Customer Data"), (ii) all intellectual property, including patents, copyrights, trademarks, trade secrets and other proprietary information ("IP") of Customer that may be made available to SecureWorks in the course of providing Services under this Agreement and (iii) all confidential or proprietary information of Customer or Customer Affiliates, including, but not limited to, Customer Data, Customer Reports, and other Customer files, documentation and related materials, in each case under this clause (iii), obtained by SecureWorks in connection with this Agreement.

During the term of the Services, Customer grants to SecureWorks a limited, non-exclusive license to use the Customer Data solely for the purposes contemplated by this Agreement and for SecureWorks to perform the Services hereunder. This Agreement does not transfer or convey to SecureWorks or any third party any right, title or interest in or to the Customer Data or any associated IP rights, but only a limited right of use as granted in and revocable in accordance with this Agreement.

k) Examination of Records and Audits

The Consultant agrees that the Cook County Auditor or any of its duly authorized representatives shall, upon reasonable advance notice, not less than thirty (30) days, until expiration of three (3) years after the final payment under the Contract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices, and records of the Consultant related to the Contract, or to Consultant's compliance with any term, condition or provision thereof. The Consultant shall be responsible for establishing and maintaining records sufficient to document the costs associated with performance under the terms of this Contract. The County's audit rights shall not include the right to audit: (i) the confidential information of SecureWorks' other customers or vendors, (ii) internal audit reports created by SecureWorks' internal audit group as part of SecureWorks' corporate internal audit function and not provided to SecureWorks' other customers generally, (iii) records regarding SecureWorks' manufacture, design and production of proprietary policies and processes used in the provision of the Services, (iv) access to SecureWorks' labs. SecureWorks shall make its operations and data centers available during normal business hours for security auditing purposes with thirty (30) days' advance written request. Any access to Consultant's sensitive facilities is strictly prohibited, in accordance with regulatory restrictions on access to data of Consultant's other customers (although a permitted auditor shall be entitled to observe the SOC via a viewing window). Consultant agrees upon providing documentation in response to an audit request to indicate if documentation is of a confidential nature and should be treated as such by the Cook County Auditor or any of its duly authorized representatives.

The Consultant agrees upon providing documentation in response to an audit request to indicate if documentation is of a confidential nature and should be treated as such by the Cook County

Auditor or any of its duly authorized representatives.

The Consultant further agrees that it shall include in all of its agreements with any Subconsultants hired to perform Services hereunder a provision that allows the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after final payment under the subcontract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices and records of such Subcontractor involving transactions relating to the subcontract, or to such Subcontractor compliance with any term, condition or provision thereunder or under this Agreement.

In the event the Contractor receives payment under this Agreement, payment for which is later disallowed by the County because the Services were not provided or the Deliverables were not delivered, the Contractor shall promptly refund any sums due to the County following the delivery of the audit results to the Contractor. The County may credit the amount disallowed from the next payment due or to become due to the Contractor under any contract with the County.

If Consultant carries out any of its duties under this Agreement through a Subconsultant involving a value of cost of \$10,000.00 or more over a 12 month period, Consultant will cause such subcontract to contain a clause to the effect that, until the expiration of three (3) years after the furnishing of any service pursuant to said subcontract, the Subconsultant will make available upon request of the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives, copies of said subcontract and any books, documents, records and other data of said related organization that are necessary to certify the nature and extent of such costs. This paragraph relating to the retention and production of documents is included because of possible application of Section 1861(v)(1)(I) of the Social Security Act to this Agreement; if this Section should be found to be inapplicable, then this paragraph shall be deemed inoperative and without force and effect.

1) Subcontracting or Assignment of Contract or Contract Funds

Once awarded, this Agreement shall not be subcontracted or assigned, in whole or in part, without the advance written approval of the Chief Procurement Officer, which approval shall not be unreasonably withheld. The Consultant shall not transfer or assign any contract funds or any interest therein due or to become due without the advance written approval of the Chief Procurement Officer. The unauthorized assignment of this Agreement, in whole or in part, or the unauthorized transfer or assignment of any contract funds, either in whole or in part, or any interest therein, which shall be due or are to become due the Consultant shall have no effect on the County and are null and void.

Prior to the commencement of this Agreement, the Consultant shall identify in writing to the Chief Procurement Officer the names of any and all Subcontractors it intends to use in the performance of this Agreement by completing the Identification of Subcontractor/Supplier/ Subconsultant Form ("ISF"). The Chief Procurement Officer shall have the right to disapprove any Subcontractor. All Subcontractors shall be subject to the terms of this Contract. Upon written request of the Chief Procurement Officer, Consultant shall provide copies of subcontracts (provided that confidential/proprietary information may be redacted) for any Subcontractors identified in the MBE/WBE Utilization Plan or any Subcontractors that are engaged specifically and solely to provide Services to the County as set forth in this Agreement as identified in the Identification of

Subcontractor/Supplier/Subconsultant Form.” The Chief Procurement Officer shall have the right to disapprove any Subcontractor. All Subcontractors shall be subject to the terms of this Contract.

The Consultant must disclose the name and business address of each Subcontractor hired by Consultant to perform Services under this Agreement, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Consultant is not required to disclose employees who are paid or estimated to be paid. The Consultant is not required to disclose employees who are paid solely through the Consultant’s regular payroll.

The Consultant must disclose the name and business address of any attorney, Lobbyist, accountant, consultant and any other person or entity whom the Consultant retains specifically to perform services for this Agreement, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Consultant is not required to disclose employees who are paid or estimated to be paid. The Consultant is not required to disclose employees who are paid solely through the Consultant’s regular payroll. “Lobbyist” means any person or entity who undertakes to influence any legislation or administrative action on behalf of any person or entity other than: (1) a not-for-profit entity, on an unpaid basis, or (2), himself. “Lobbyist” also means any person or entity any part of whose duties as an employee of another includes undertaking to influence any legislative or administrative action. If the Consultant is uncertain whether a disclosure is required under this Section, the Consultant must either ask the County, whether disclosure is required or make the disclosure.

The County reserves the right to prohibit any person from entering any County facility for any reason. All Consultants and Subcontractors of the Consultant shall be accountable to the Chief Procurement Officer or his designee while on any County property and shall abide by all rules and regulations imposed by the County.

m) Limitation of Liability

- i) NEITHER THE SECUREWORKS PARTIES NOR CUSTOMER WILL BE LIABLE FOR ANY INCIDENTAL, INDIRECT, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT. NOTWITHSTANDING THE FOREGOING, NEITHER PARTY SHALL HAVE ANY LIABILITY FOR THE FOLLOWING: (A) LOSS OF REVENUE, INCOME, PROFIT, OR SAVINGS, (B) LOST OR CORRUPTED DATA OR SOFTWARE, LOSS OF USE OF SYSTEM(S) OR NETWORK, OR THE RECOVERY OF SUCH, (C) LOSS OF BUSINESS OPPORTUNITY, OR (D) BUSINESS INTERRUPTION OR DOWNTIME.
- ii) EXCEPT FOR CLAIMS ARISING FROM THE WILLFUL MISCONDUCT OR GROSS NEGLIGENCE OF A PARTY, OR A PARTY’S UNAUTHORIZED USE OR DISCLOSURE OF THE OTHER PARTY’S CONFIDENTIAL INFORMATION IN BREACH OF ARTICLE 3(H) (IT BEING UNDERSTOOD AND AGREED THAT ANY UNAUTHORIZED INTRUSION INTO A NETWORK AND ACCESS TO CONFIDENTIAL INFORMATION BY A THIRD PARTY (E.G., A ‘HACK’) WILL NOT CONSTITUTE AN UNAUTHORIZED USE OR DISCLOSURE OF CONFIDENTIAL INFORMATION FOR THIS PURPOSE), NEITHER PARTY’S AGGREGATE LIABILITY FOR ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT SHALL EXCEED TWO (2) TIMES THE AMOUNTS PAID OR PAYABLE BY CUSTOMER FOR THE SERVICES

PROVIDED DURING THE TWELVE (12) MONTH PERIOD PRIOR TO SUCH CLAIM (excludes gross negligence/willful misconduct, bodily injury or death/property damage, and confidentiality/security breaches);

- iii) The foregoing limitations, exclusions and disclaimers shall apply, regardless of whether the claim for such damages is based in contract, warranty, strict liability, negligence, and tort or otherwise. Insofar as applicable law prohibits any limitation herein, the parties agree that such limitation will be automatically modified, but only to the extent so as to make the limitation permitted to the fullest extent possible under such law.

ARTICLE 4) TERM OF PERFORMANCE

a) Term of Performance

This Agreement takes effect when approved by the Cook County Board and its term shall begin on July 13, 2016 ("**Effective Date**") and continue until July 12, 2019 or until this Agreement is terminated in accordance with its terms, whichever occurs first.

b) Timeliness of Performance

- i) Consultant must provide the Services and Deliverables within the term and within the time limits required under this Agreement, pursuant to the provisions of Section 4.a and Exhibit 1.
- ii) Neither Consultant nor Consultant's agents, employees nor Subcontractors are entitled to any damages from the County, nor is any party entitled to be reimbursed by the County, for damages, charges or other losses or expenses incurred by Consultant by reason of delays or hindrances in the performance of the Services, whether or not caused by the County. SecureWorks will be granted a reasonable extension to perform its obligations under this Agreement to the extent such failure is caused solely by Customer's delay in performing or failure to perform its responsibilities under this Agreement and/or the applicable Service Order/SOW.

c) Agreement Extension Option

The Chief Procurement Officer may at any time before this Agreement expires elect to renew this Agreement for up to two (2) additional one-year renewal periods under the same terms and conditions as this original Agreement, except as provided otherwise in this Agreement, by notice in writing to Consultant. After notification by the Chief Procurement Officer, this Agreement must be modified to reflect the time extension in accordance with the provisions of Section 10.c.

ARTICLE 5) COMPENSATION

a) Basis of Payment

The County will pay Consultant according to the Schedule of Compensation in the applicable Service Order or SOW. If no Schedule of Compensation is included, then (i) all charges, fees, payments and amounts hereunder will be in United States dollars, and (ii) all undisputed amounts

due hereunder are payable within forty-five (45) days from the date of the invoice, which shall be submitted to Customer electronically, (the "Invoice Due Date").

b) Method of Payment

All invoices submitted by the Consultant shall be in accordance with the cost provisions contained in the Agreement and shall contain a description of the Products/Services, including, if applicable, the quantity of the Products/Services, for which payment is requested. All invoices for Consulting Services shall include, if applicable, itemized entries indicating the date or time period in which the services were provided, the amount of time spent performing the services, and a detailed description of the services provided during the period of the invoice. Invoices for new charges shall not include "past due" amounts, if any, which amounts must be set forth on a separate invoice. Consultant shall not be entitled to invoice the County for any late fees or other penalties.

In accordance with Section 34-177 of the Cook County Procurement Code, the County shall have a right to set off and subtract from any invoice(s) or contract price, a sum equal to any fines and penalties, including interest, for any tax or fee delinquency and any debt or obligation owed by the Consultant to the County.

The Consultant acknowledges its duty to ensure the accuracy of all invoices submitted to the County for payment. By submitting the invoices, the Consultant certifies that all itemized entries set forth in the invoices are true and correct. The Consultant acknowledges that by submitting the invoices, it certifies that it has delivered the Deliverables, i.e., the goods, supplies, services or equipment set forth in the Agreement to the Using Agency, or that it has properly performed the services set forth in the Agreement. The invoice must also reflect the dates and amount of time expended in the provision of services under the Agreement. The Consultant acknowledges that any inaccurate statements or negligent or intentional misrepresentations in the invoices shall result in the County exercising all remedies available to it in law and equity including, but not limited to, a delay in payment or non-payment to the Consultant, and reporting the matter to the Cook County Office of the Independent Inspector General.

When Consultant receives any payment from the County for the Services provided to the County pursuant to its Agreement, the Consultant must make payment to any of its Subcontractors that are engaged specifically and solely to provide Services to the County as set forth in this Agreement, within fifteen (15) days after receipt of payment from the County, provided that such Subcontractor has satisfactorily provided the supplies, equipment, goods or services in accordance with this Agreement and has provided the Consultant with all of the documents and information required by the Consultant. The Consultant may delay or postpone payment to a Subcontractor when the Subcontractor's supplies, equipment, goods, or services do not comply with the requirements of this Agreement, the Consultant is acting in good faith, and not in retaliation for a Subcontractor exercising legal or contractual rights.

c) Funding

The source of funds for payments under this Agreement is identified in Exhibit 2, Schedule of Compensation. Payments under this Agreement must not exceed the dollar amount shown in Exhibit 2 without a written amendment in accordance with Section 10.c.

d) Non-Appropriation

If no funds or insufficient funds are appropriated and budgeted in any fiscal period of the County for payments to be made under this Agreement, then the County will notify Consultant in writing of that occurrence, and this Agreement will terminate on the earlier of the last day of the fiscal period for which sufficient appropriation was made or whenever the funds appropriated for payment under this Agreement are exhausted. Payments for Services completed to the date of notification will be made to Consultant. No payments will be made or due to Consultant and under this Agreement beyond those amounts appropriated and budgeted by the County to fund payments under this Agreement.

e) Taxes

Federal Excise Tax does not apply to materials purchased by the County by virtue of Exemption Certificate No. 36-75-0038K. Illinois Retailers' Occupation Tax, Use Tax and Municipal Retailers' Occupation Tax do not apply to deliverables, materials or services purchased by the County by virtue of statute. The price or prices quoted herein shall include any and all other federal and/or state, direct and/or indirect taxes which apply to this Agreement. The County's State of Illinois Sales Tax Exemption Identification No. is E-9998-2013-07.

f) Nonpayment

Customer shall have the right to reasonably, and in good faith, dispute any invoice or any portion of any invoice claimed by SecureWorks as due and payable provided that, prior to the Invoice Due Date, Customer (i) timely pays any undisputed portion of the amount, due and payable, and (ii) provides SecureWorks with written notice specifying the disputed amount and the basis for the dispute in reasonable detail. In addition, SecureWorks, without waiving any other rights or remedies to which it may be entitled, shall have the right, upon prior written notice to Customer, to suspend the Services until such payment is received.

ARTICLE 6) DISPUTES

Any dispute arising under this Agreement between the County and Consultant shall be decided by the Chief Procurement Officer. The complaining party shall submit a written statement detailing the dispute and specifying the specific relevant contract provision(s) to the Chief Procurement Officer. Upon request of the Chief Procurement Officer, the party complained against shall respond to the complaint in writing within five days of such request. The Chief Procurement Officer will reduce her decision to writing and mail or otherwise furnish a copy thereof to the Consultant. The decision of the Chief Procurement Officer will be final and binding. Dispute resolution as provided herein shall be a condition precedent to any other action at law or in equity. However, unless a notice is issued by the Chief Procurement Officer indicating that additional time is required to review a dispute, the parties may exercise their contractual remedies, if any, if no decision is made within sixty (60) days following notification to the Chief Procurement Officer of a dispute. No inference shall be drawn from the absence of a decision by the Chief Procurement Officer

Notwithstanding a dispute, except for dispute relating to the County's payment obligations, each party shall continue to discharge all its obligations, duties and responsibilities set forth in this Agreement during any dispute resolution proceeding unless otherwise agreed to by the County in writing. If Consultant finds the county in default, consultant will provide written notice that County has sixty (60) days to remediate before termination of contract.

ARTICLE 7) COOPERATION WITH INSPECTOR GENERAL AND COMPLIANCE WITH ALL LAWS

The Consultant, Subcontractor, licensees, grantees or persons or businesses who have a County contract, grant, license, or certification of eligibility for County contracts shall abide by all of the applicable provisions of the Office of the Independent Inspector General Ordinance (Section 2-281 et. seq. of the Cook County Code of Ordinances). Failure to cooperate as required may result in monetary and/or other penalties.

The Consultant shall observe and comply with the laws, ordinances, regulations and codes of the Federal, State, County and other local government agencies which may in any manner affect the performance of this Agreement including, but not limited to, those County Ordinances set forth in the Certifications attached hereto and incorporated herein. Assurance of compliance with this requirement by the Consultant's employees, agents or Subcontractor shall be the responsibility of the Consultant.

The Consultant shall secure and pay for all federal, state and local licenses, permits and fees required for Consultant's Services hereunder.

ARTICLE 8) SPECIAL CONDITIONS

a) Warranties and Representations

In connection with signing and carrying out this Agreement, Consultant:

- i) warrants that Consultant is appropriately licensed to perform the Services required under this Agreement and will perform no Services for which a professional license is required by law and for which Consultant is not appropriately licensed;
- ii) warrants it is financially solvent; it and each of its employees, agents and Subcontractors of any tier are competent to perform the Services required under this Agreement; and Consultant is legally authorized to execute and perform or cause to be performed this Agreement under the terms and conditions stated in this Agreement;
- iii) warrants that it will not knowingly use the services of any ineligible consultant or Subcontractor for any purpose in the performance of its Services under this Agreement;
- iv) warrants that Consultant or Subcontractor is not in default at the time this Agreement is signed, and has not been considered by the Chief Procurement Officer to have, within five (5) years immediately preceding the date of this Agreement, been found to be in default on any contract awarded by the County;
- v) represents that it has carefully examined and analyzed the provisions and requirements of this Agreement; it understands the nature of the Services required; from its own analysis it has satisfied itself as to the nature of all things needed for the performance of this Agreement; this Agreement is feasible of performance in accordance with all of its provisions and requirements, and Consultant warrants it can and will perform, or cause to be performed, the Services in accordance with the provisions and requirements of this Agreement;

- vi) represents that Consultant and, to the best of its knowledge, its Subcontractors are not in violation of the provisions of the Illinois Criminal Code, 720 ILCS 5/33E as amended; and
- vii) acknowledges that any certification, affidavit or acknowledgment made under oath in connection with this Agreement is made under penalty of perjury and, if false, is also cause for termination under Sections 9.a and 9.c.

b) Ethics

- i) In addition to the foregoing warranties and representations, Consultant warrants:
 - (1) no officer, agent or employee of the County is employed by Consultant or has a financial interest directly or indirectly in this Agreement or the compensation to be paid under this Agreement except as may be permitted in writing by the Board of Ethics.
 - (2) no payment, gratuity or offer of employment will be made in connection with this Agreement by or on behalf of Consultant or any Subcontractors or anyone associated with them, as an inducement for the award of a subcontract or order.

c) Business Documents

At the request of the County, Consultant must provide corporate documents which provide that the person executing this Agreement has the authority to bind the Consultant.

d) Conflicts of Interest

- i) No member of the governing body of the County or other unit of government and no other officer, employee or agent of the County or other unit of government who exercises any functions or responsibilities in connection with the Services to which this Agreement pertains is permitted to have any personal interest, direct or indirect, in this Agreement. No member of or delegate to the Congress of the United States or the Illinois General Assembly and no Commissioner of the Cook County Board or County employee is allowed to be admitted to any share or part of this Agreement or to any financial benefit to arise from it.
- ii) Consultant covenants that it, and to the best of its knowledge, its Subcontractors if any (collectively, "**Consulting Parties**"), presently have no direct or indirect interest and will not acquire any interest, direct or indirect, in any project or contract that would conflict in any manner or degree with the performance of its Services under this Agreement.
- iii) If Consultant becomes aware of a conflict, it must immediately stop work on the assignment causing the conflict and notify the County.
- iv) Without limiting the foregoing, if the Consulting Parties assist the County in determining the advisability or feasibility of a project or in recommending, researching, preparing,

drafting or issuing a request for proposals or bid specifications for a project, the Consulting Parties must not participate, directly or indirectly, as a prime, Subcontractor or joint venturer in that project or in the preparation of a proposal or bid for that project during the term of this Agreement or afterwards. The Consulting Parties may, however, assist the County in reviewing the proposals or bids for the project if none of the Consulting Parties have a relationship with the persons or entities that submitted the proposals or bids for that project.

- v) The Consultant further covenants that, in the performance of this Agreement, no person having any conflicting interest will be assigned to perform any Services or have access to any confidential information, as defined in Section 3.h of this Agreement. If the County, by the Chief Procurement Officer in his reasonable judgment, determines that any of Consultant's Services for others conflict with the Services Consultant is to render for the County under this Agreement, County may immediately terminate this Agreement pursuant to 9a and 9c.
- vi) Furthermore, if any federal funds are to be used to compensate or reimburse Consultant under this Agreement, Consultant represents that it is and will remain in compliance with federal restrictions on lobbying set forth in Section 319 of the Department of the Interior and Related Agencies Appropriations Act for Fiscal year 1990, 31 U.S.C. § 1352, and related rules and regulations set forth at 54 Fed. Reg. 52,309 ff. (1989), as amended. If federal funds are to be used, Consultant must execute a Certification Regarding Lobbying, which will be attached as an exhibit and incorporated by reference as if fully set forth here.

e) Non-Liability of Public Officials

Consultant and any assignee or Subcontractor of Consultant must not charge any official, employee or agent of the County personally with any liability or expenses of defense or hold any official, employee or agent of the County personally liable to them under any term or provision of this Agreement or because of the County's execution, attempted execution or any breach of this Agreement.

**ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION
AND RIGHT TO OFFSET**

a) Events of Default Defined

The following constitute events of default:

- i) Any material misrepresentation, whether negligent or willful and whether in the inducement or in the performance, made by one party to the other.
- ii) Any material failure of a party to perform any of its obligations under this Agreement, and such default continues un-remedied for a period of sixty (60) days following written notice of default, including the following:
 - (a) Consultant's material failure to perform the Services in accordance with the terms and conditions of this Agreement or inability to perform the Services

satisfactorily as a result of insolvency, filing for bankruptcy or assignment for the benefit of creditors;

- (b) Failure to promptly re-perform within a reasonable time Services that were rejected as erroneous or unsatisfactory;
 - (c) Consultant's discontinuance of the Services for reasons within Consultant's reasonable control; and
 - (d) A party's material failure to comply with any other material term of this Agreement, including the provisions concerning insurance, confidentiality and ownership of documents, intellectual property and nondiscrimination.
- iii) Any change in ownership or control of Consultant without the prior written approval of the Chief Procurement Officer, which approval the Chief Procurement Officer will not unreasonably withhold.
 - iv) Consultant's default under any other agreement it may presently have or may enter into with the County during the life of this Agreement. Consultant acknowledges and agrees that in the event of a default under this Agreement the County may also declare a default under any such other Agreements.
 - v) Failure to comply with Article 7 in the performance of the Agreement.
 - vi) Consultant's repeated or continued violations of County ordinances unrelated to performance under the Agreement that in the opinion of the Chief Procurement Officer indicate a willful or reckless disregard for County laws and regulations.

b) Remedies

The occurrence of any event of default permits the non-defaulting, at the non-defaulting party's sole option, to declare the other party in default. The Chief Procurement Officer may in his sole discretion give Consultant an opportunity to cure the default within a certain period of time, which period of time must not exceed 30 days, unless extended by the Chief Procurement Officer. Consultant shall in its sole discretion give the County an opportunity to cure the default within a certain period of time, which period of time must not exceed 30 days, unless extended by Consultant. Whether to declare a party in default is within the sole discretion of the non-defaulting party and neither that decision nor the factual basis for it is subject to review or challenge under the Disputes provision of this Agreement.

The Chief Procurement Officer will give Consultant written notice of the default, either in the form of a cure notice ("**Cure Notice**"), or, if no opportunity to cure will be granted, a default notice ("**Default Notice**"). If the Chief Procurement Officer gives a Default Notice, he will also indicate any present intent he may have to terminate this Agreement, and the decision to terminate (but not the decision not to terminate) is final and effective upon giving the notice. The Chief Procurement Officer may give a Default Notice if Consultant fails to affect a cure within the cure period given in a Cure Notice. When a Default Notice with intent to terminate is given as provided in this Section 9.b and Article 11, Consultant must discontinue any Services,

unless otherwise directed in the notice, and deliver all materials accumulated in the performance of this Agreement, whether completed or in the process, to the County. After giving a Default Notice, the County may invoke any or all of the following remedies:

- i) The right to terminate this Agreement as to any or all of the Services yet to be performed effective at a time specified by the County;
- ii) The right of specific performance, an injunction or any other appropriate equitable remedy;
- iii) The right to money damages;
- iv) The right to withhold all or any part of Consultant's compensation under this Agreement;
- v) The right to consider Consultant non-responsible in future contracts to be awarded by the County.

If the Chief Procurement Officer considers it to be in the County's best interests, he may elect not to declare default or to terminate this Agreement. The parties acknowledge that if the County permits Consultant to continue to provide the Services despite one or more events of default, Consultant is in no way relieved of any of its responsibilities, duties or obligations under this Agreement, nor does the County waive or relinquish any of its rights.

The remedies under the terms of this Agreement are not intended to be exclusive of any other remedies provided, but each and every such remedy is cumulative and is in addition to any other remedies, existing now or later, at law, in equity or by statute. No delay or omission to exercise any right or power accruing upon any event of default impairs any such right or power, nor is it a waiver of any event of default nor acquiescence in it, and every such right and power may be exercised from time to time and as often as the party considers expedient.

c) Early Termination

In addition to termination under Sections 9.a and 9.b of this Agreement, the County may terminate this Agreement, or all or any portion of the Services to be performed under it, at any time by a notice in writing from the County to Consultant. The County will give notice to Consultant in accordance with the provisions of Article 11. The effective date of termination will be the date the notice is received by Consultant or the date stated in the notice, whichever is later. If the County elects to terminate this Agreement in full, all Services to be provided under it must cease and all materials that may have been accumulated in performing this Agreement, whether completed or in the process, must be delivered to the County effective 10 days after the date the notice is considered received as provided under Article 11 of this Agreement (if no date is given) or upon the effective date stated in the notice.

After the notice is received, Consultant must restrict its activities, and those of its Subcontractors, to winding down any reports, analyses, or other activities previously begun. No costs incurred after the effective date of the termination are allowed. Payment for any Services actually and satisfactorily performed before the effective date of the termination is on the same basis as set forth in Article 5, but if any compensation is described or provided for on the basis of

a period longer than 10 days, then the compensation must be prorated accordingly. No amount of compensation, however, is permitted for anticipated profits on unperformed Services. The County and Consultant must attempt to agree on the amount of compensation to be paid to Consultant, but if not agreed on, the dispute must be settled in accordance with Article 6 of this Agreement. The payment so made to Consultant is in full settlement for all Services satisfactorily performed under this Agreement.

Consultant must include in its contracts with Subcontractors an early termination provision in form and substance equivalent to this early termination provision to prevent claims against the County arising from termination of subcontracts after the early termination. Consultant will not be entitled to make any early termination claims against the County resulting from any Subcontractor's claims against Consultant or the County to the extent inconsistent with this provision.

If the County's election to terminate this Agreement for default under Sections 9.a and 9.b is determined in a court of competent jurisdiction to have been wrongful, then in that case the termination is to be considered to be an early termination under this Section 9.c.

If this Agreement or any active Service Order and/or SOW is terminated by Customer prior to the Service term expiration date, for any reason other than SecureWorks' breach, Customer agrees to pay to SecureWorks: (i) for the Consulting Services, all unpaid Consulting Service fees as set forth on the applicable SOW for the Consulting Services performed through the effective termination date; or (ii) for MSS Services, all unpaid MSS Service fees as set forth on the applicable Service Order for the MSS Services performed through the effective termination date.

d) Suspension

The County may at any time request that Consultant suspend its Services, or any part of them, by giving fifteen (15) calendar days prior written notice to Consultant, or in the event of emergency, upon notice as soon as practicable after occurrence of the emergency. No new costs incurred after the effective date of such suspension are allowed. Consultant must promptly resume its performance of the Services under the same terms and conditions as stated in this Agreement upon written notice by the Chief Procurement Officer and such equitable extension of time as may be mutually agreed upon by the Chief Procurement Officer and Consultant when necessary for continuation or completion of Services. Any additional costs or expenses actually incurred by Consultant as a result of recommencing the Services must be treated in accordance with the compensation provisions under Article 5 of this Agreement.

No suspension of this Agreement is permitted in the aggregate to exceed a period of forty-five (45) calendar days within any twelve (12) month period of this Agreement. If the total number of days of suspension exceeds forty-five (45) calendar days, Consultant by written notice may treat the suspension as an early termination of this Agreement under Section 9.c.

e) Right to Offset

In connection with performance under this Agreement, the County may offset any excess costs incurred:

- i) if the County terminates this Agreement for Consultant's material default;

- ii) if the County exercises any of its remedies under Section 9.b of this Agreement;
or
- iii) if the County has any credits due or has made any overpayments under this Agreement.

The County may offset these excess costs by use of any payment due for Services completed before the County terminated this Agreement or before the County exercised any remedies. This right to offset is in addition to and not a limitation of any other remedies available to the County.

f) Delays

Consultant agrees that no charges or claims for damages shall be made by Consultant for any delays or hindrances from any cause whatsoever during the progress of any portion of this Agreement. SecureWorks will be granted a reasonable extension to perform its obligations under this Agreement to the extent such failure is caused solely by Customer's delay in performing or failure to perform its responsibilities under this Agreement and/or the applicable Service Order/SOW. Such extension shall not exceed 30 days from the time the County cures its delayed performance.

g) Prepaid Fees

To the extent that Customer has prepaid any Service fees, SecureWorks shall refund to Customer any prepaid Service fees on a pro-rata basis to the extent such Service fees are attributable to the period after such termination date and all amounts prepaid for Services not actually provided as of the effective date of termination. The refund shall be made within forty-five (45) days of the effective date of termination.

ARTICLE 10) GENERAL CONDITIONS

a) Entire Agreement

i) General

This Agreement, and the exhibits attached to it and incorporated in it, constitute the entire agreement between the parties and no other warranties, inducements, considerations, promises or interpretations are implied or impressed upon this Agreement that are not expressly addressed in this Agreement.

ii) No Collateral Agreements

Consultant acknowledges that, except only for those representations, statements or promises expressly contained in this Agreement and any exhibits attached to it and incorporated by reference in it, no representation, statement or promise, oral or in writing, of any kind whatsoever, by the County, its officials, agents or employees, has induced Consultant to enter into this Agreement or has been relied upon by Consultant.

iii) No Omissions

Each party acknowledges that it was given an opportunity to review all documents forming this Agreement before signing this Agreement in order that it might request inclusion in this Agreement of any statement, representation, promise or provision that it desired or on that it wished to place reliance. Each party did so review those documents, and either every such statement, representation, promise or provision has been included in this Agreement or else, if omitted, each party relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Agreement in its entirety without claiming reliance on it or making any other claim on account of its omission.

b) Counterparts

This Agreement is comprised of several identical counterparts, each to be fully signed by the parties and each to be considered an original having identical legal effect.

c) Contract Amendments

The parties may during the term of this Agreement make amendments to this Agreement but only as provided in this section. Such amendments shall only be made by mutual agreement in writing.

In the case of contracts not approved by the Board, the Chief Procurement Officer may amend a contract provided that any such amendment does not extend the Contract by more than one (1) year, and further provided that the total cost of all such amendments does not increase the total amount of the Contract beyond \$150,000. Such action may only be made with the advance written approval of the Chief Procurement Officer. If the amendment extends the Contract beyond one (1) year or increases the total award amount beyond \$150,000, then Board approval will be required.

No Using Agency or employee thereof has authority to make any amendments to this Agreement. Any amendments to this Agreement made without the express written approval of the Chief Procurement Officer is void and unenforceable.

Consultant is hereby notified that, except for amendments which are made in accordance with this Section 10.c. Contract Amendments, no Using Agency or employee thereof has authority to make any amendment to this Agreement.

d) Governing Law and Jurisdiction

This Agreement shall be governed by and construed under the laws of the State of Illinois. The Consultant irrevocably agrees that, subject to the County's sole and absolute election to the contrary, any action or proceeding in any way, manner or respect arising out of this Agreement, or arising from any dispute or controversy arising in connection with or related to this Agreement, shall be litigated only in courts within Cook County, State of Illinois, and the Consultant consents and submits to the jurisdiction thereof. In accordance with these provisions, Consultant waives any right it may have to transfer or change the venue of any litigation brought against it by the County pursuant to this Agreement.

e) Severability

If any provision of this Agreement is held or considered to be or is in fact invalid, illegal, inoperative or unenforceable as applied in any particular case in any jurisdiction or in all cases because it conflicts with any other provision or provisions of this Agreement or of any constitution, statute, ordinance, rule of law or public policy, or for any other reason, those circumstances do not have the effect of rendering the provision in question invalid, illegal, inoperative or unenforceable in any other case or circumstances, or of rendering any other provision or provisions in this Agreement invalid, illegal, inoperative or unenforceable to any extent whatsoever. The invalidity, illegality, inoperativeness or unenforceability of any one or more phrases, sentences, clauses or sections in this Agreement does not affect the remaining portions of this Agreement or any part of it.

f) Assigns

All of the terms and conditions of this Agreement are binding upon and inure to the benefit of the parties and their respective legal representatives, successors and assigns.

g) Cooperation

Consultant must at all times cooperate fully with the County and act in the County's best interests. If this Agreement is terminated for any reason, or if it is to expire on its own terms, Consultant must make every effort to assure an orderly transition to another provider of the Services, if any, orderly demobilization of its own operations in connection with the Services, uninterrupted provision of Services during any transition period and must otherwise comply with the reasonable requests and requirements of the Using Agency in connection with the termination or expiration.

Customer Cooperation. Customer acknowledges that SecureWorks' performance and delivery of the Services are contingent upon: (A) Customer providing safe and hazard-free access to its personnel, facilities, equipment, hardware, network and information, and (B) Customer's timely decision-making, providing the requested information and granting of approvals or permissions, as (A) and (B) are deemed reasonably necessary and reasonably requested for SecureWorks to perform, deliver and/or implement the Services. Customer will promptly obtain and provide to SecureWorks any required licenses, approvals or consents necessary for SecureWorks' performance of the Services. SecureWorks will be excused from its failure to perform its obligations under this Agreement to the extent such failure is caused solely by Customer's delay in performing or failure to perform its responsibilities under this Agreement and/or the applicable Service Order/SOW, including but not limited to, any applicable SLAs thereto.

h) Waiver

Nothing in this Agreement authorizes the waiver of a requirement or condition contrary to law or ordinance or that would result in or promote the violation of any federal, state or local law or ordinance.

Whenever under this Agreement the County by a proper authority waives Consultant's performance in any respect or waives a requirement or condition to either the County's or Consultant's performance, the waiver so granted, whether express or implied, only applies to the particular instance and is not a waiver forever or for subsequent instances of the performance, requirement or condition. No such waiver is a modification of this Agreement regardless of the

number of times the County may have waived the performance, requirement or condition. Such waivers must be provided to Consultant in writing.

i) Independent Consultant

This Agreement is not intended to and will not constitute, create, give rise to, or otherwise recognize a joint venture, partnership, corporation or other formal business association or organization of any kind between Consultant and the County. The rights and the obligations of the parties are only those expressly set forth in this Agreement. Consultant must perform under this Agreement as an independent Consultant and not as a representative, employee, agent, or partner of the County.

This Agreement is between the County and an independent Consultant and, if Consultant is an individual, nothing provided for under this Agreement constitutes or implies an employer-employee relationship such that:

- i) The County will not be liable under or by reason of this Agreement for the payment of any compensation award or damages in connection with the Consultant performing the Services required under this Agreement.
- ii) Consultant is not entitled to membership in the County Pension Fund, Group Medical Insurance Program, Group Dental Program, Group Vision Care, Group Life Insurance Program, Deferred Income Program, vacation, sick leave, extended sick leave, or any other benefits ordinarily provided to individuals employed and paid through the regular payrolls of the County.
- iv) The County is not required to deduct or withhold any taxes, FICA or other deductions from any compensation provided to the Consultant.

j) Governmental Joint Purchasing Agreement

Pursuant to Section 4 of the Illinois Governmental Joint Purchasing Act (30 ILCS 525) and the Joint Purchase Agreement approved by the Cook County Board of Commissioners (April 9, 1965), other units of government may purchase goods or services under this Agreement.

In the event that other agencies participate in a joint procurement, the County reserves the right to renegotiate the price to accommodate the larger volume.

k) Comparable Government Procurement

As permitted by the County of Cook, other government entities, if authorized by law, may wish to purchase the goods, supplies, services or equipment under the same terms and conditions contained in this Agreement (i.e., comparable government procurement). Each entity wishing to reference this Agreement must have prior authorization from the County of Cook and the Consultant. If such participation is authorized, all purchase orders will be issued directly from and shipped directly to the entity requiring the goods, supplies, equipment or services supplies/services. The County shall not be held responsible for any orders placed, deliveries made or payment for the goods, supplies, equipment or services supplies/services ordered by

these entities. Each entity reserves the right to determine the amount of goods, supplies, equipment or services it wishes to purchase under this Agreement.

l) Force Majeure

Neither Consultant nor County shall be liable for failing to fulfill any obligation under this Agreement if such failure is caused by an event beyond such party's reasonable control and which is not caused by such party's fault or negligence. Such events shall be limited to acts of God, acts of war, fires, lightning, floods, epidemics, or riots.

ARTICLE 11) NOTICES

All notices required pursuant to this Agreement shall be in writing and addressed to the parties at their respective addresses set forth below. All such notices shall be deemed duly given if hand delivered or if deposited in the United States mail, postage prepaid, registered or certified, return receipt requested. Notice as provided herein does not waive service of summons or process.

If to the County: Department of Homeland Security and Emergency Management
69 W. Washington, Suite 2600
Chicago, Illinois 60602
Attention: Department Director

and

Cook County Chief Procurement Officer
118 North Clark Street, Room 1018
Chicago, Illinois 60602
(Include County Contract Number on all notices)

If to Consultant: SecureWorks, Inc.
One Concourse Parkway, Suite 500
Atlanta, GA 30328
Attention: Legal

Changes in these addresses must be in writing and delivered in accordance with the provisions of this Article 11. Notices delivered by mail are considered received three days after mailing in accordance with this Article 11. Notices delivered personally are considered effective upon receipt. Refusal to accept delivery has the same effect as receipt.

ARTICLE 12) AUTHORITY

Execution of this Agreement by Consultant is authorized by a resolution of its Board of Directors, if a corporation, or similar governing document, and the signature(s) of each person signing on behalf of Consultant have been made with complete and full authority to commit Consultant to all terms and conditions of this Agreement, including each and every representation, certification and warranty contained in it, including the representations, certifications and warranties collectively incorporated by reference in it.

EXHIBIT 1

Scope of Services

STATEMENT OF WORK NUMBER C-20160407-0001

This Statement of Work ("SOW") is entered into by and between SecureWorks, Inc., with its principal place of business located at One Concourse Parkway, Suite 500, Atlanta, GA 30328 ("SecureWorks") and County of Cook with its principal place of business located at 69 W Washington, Chicago, IL 60602 ("Customer") as of July 15th, 2016, which is defined in the Professional Services Agreement. SecureWorks and Customer hereafter referred to together as the "parties", or individually as "party". This SOW is governed by and subject to the terms and conditions of: (a) the separately signed Professional Services Agreement executed by the parties that expressly authorizes Customer to order the services described herein from SecureWorks, Capitalized terms not defined herein shall have the meaning ascribed to them in the MSA.

1 Services Overview

SecureWorks will provide Customer with a comprehensive set of Monitored and Professional Security Services, listed below, to enhance Customer's security posture. As part of those services, SecureWorks will ensure the successful stand up and tuning for all Monitored Security Services (MSS). Following is an overview of each service in scope.

1.1 Customer Transition Services Scope


The following Customer Transition Services (CTS) components are performed by the transition program manager (Conduct planning, review, and governance meetings and work sessions





1.2 **MSSI+ Scope**

Under this Statement of Work (SOW), SecureWorks will provide Customer with Managed Security Services Integration Plus (MSSI+) services worth seven (7) weeks of effort, to be paid by Customer as set forth and determined below.



1.3 **Monitored Security Services**

Please refer to Exhibit C

1.4 **Threat Intelligence Services**

Please refer to Exhibit D

1.5 **Device Management**

Please refer to Exhibit E

1.6 **Service Delivery Executive**

SecureWorks Service Delivery Executives (SDE) are both professional and technical service leaders responsible for optimizing client value through the delivery of SecureWorks services for critical enterprise clients. The Service Delivery Executive develops a deep understanding of the client's day-to-day operation and how it applies to the applicable service delivery to insure optimal workflow is achieved. The key responsibility of the Service Delivery Executive is to support continual service

improvement and client satisfaction as well as playing a strategic role in ensuring the highest level of operational service delivery. The SDE is assigned as a leveraged resource, shared with other accounts.

Core responsibilities of the SDE include:

[REDACTED]

1.7 Incident Management Retained Services Scope

The Incident Management Retained Services that SecureWorks offers provides the full spectrum of use cases and capability maturity for Incident Management. Customer agrees to the purchase of a block of hours as set forth in Section 5.10 below (*Service Fees and Expenses - Incident Management Retained Services*) ("Retained Hours") from SecureWorks to be utilized for one or more SecureWorks proactive or reactive Incident Management Services at Customer's choosing and as further described below in Appendix F - Incident Management Retained Services with a commitment from SecureWorks to a response time for reactive Incident Management Services.

[REDACTED]



2 Location of Services

The MSS Services listed in Exhibits C through E shall be performed remotely at one or more SecureWorks secure operation centers (“SOC(s)”). Located within the United States for Affiliates.

Through the use of role-based access controls, SecureWorks will ensure that access to Customer's security events and security ticketing is limited to CTOC personnel in the US and the UK (Edinburgh Scotland). Health events and Health ticketing may be supported by staff located in secure facilities outside of the U.S. Data is stored in datacenters in two locations within the United States.

Data is viewed from the following locations:

US (All Services)

Hyderabad India (Health team)

Edinburgh Scotland (Device Management, VMS, CTAC, Health)

All other Services may be performed either onsite at the Customer location defined below and/or remotely at one or more SecureWorks secure facilities. SecureWorks and Customer will determine the location of the performance of the Services to be performed hereunder. In most cases, the collection of the required Customer Data will be gathered onsite and the drafting of the Report (as defined below) and recommendations will be built remotely.

Customer Location:

Primary:

69 W Washington

Chicago, IL 60602

Alternate: Cook County Facilities within Cook County

3 Timeline and Services Schedules

- For timelines of MSS, please refer to Exhibits C through E
- For all other Services
 - Onsite Consulting work will be performed Monday-Friday, 8 am - 6 pm Local time.
 - Remote Consulting work will occur Monday-Friday, 8 am - 5 pm for the assigned resource(s)
- Work performed outside of the hours listed in this SOW as requested or required by Customer will incur additional Service charges. Authorization must be provided in writing by client CISO.

4 Service Details

Under this SOW, SecureWorks will provide Customer with the following list of services (“Services”), as such services are described in the corresponding Exhibits at the end of this document:

- Exhibit A - Customer Transition Services
- Exhibit B - MSS Integration Plus -7 Weeks
- Exhibit C - Monitored Security Services
- Exhibit D - Threat Intelligence Services
- Exhibit E - Device Management
- Exhibit F - Incident Management Retained Services

5 Service Fees and Expenses

The following tables represent the agreed upon pricing for the Services, valid for the term of the Agreement. Note: all amounts are in USD, exclusive of taxes and other applicable fees including any shipping and handling. All Devices in scope are assumed to be in SecureWorks-approved service areas/geographies. All Service Terms and Service Level Agreements defined in Exhibits C, D, and E apply.

5.1 MSS: Server Monitoring

Services for Security Monitoring, described in Exhibit C, is based on fixed fees for a range of server device quantities monitored by SecureWorks. All devices must be on the SecureWorks supported Server Monitoring list and located within supported global geographies. Includes 24x7x365 log monitoring/correlation/alerting for these devices.

Upon activation of the first set of devices, COOK COUNTY will be invoiced and required to pay for the full range. Customer acknowledges that the Service Fees due SecureWorks per the terms of this Section are for the capacity of device quantities stated during the Services Term, whether or not such capacity is ever fully utilized.

5.2 MSS: Firewall Monitoring

A "Basic Firewall" is defined as a device that only acts as a firewall. A "Next Generation Firewall" is defined as device that has "Basic Firewall" functionality plus any other capabilities such as: IDS/IPS, URL content filtering, gateway antivirus, etc. An active-standby HA "Basic Firewall" device pair counts as 1 device. All devices must be on the SecureWorks supported Monitored Firewall list and located within supported global geographies. Excludes any Web Application Firewalls (WAFs) or Database-specific Firewalls which can be quoted separately. Excludes management of any "Basic Firewall" or "Next Generation Firewall" devices - only includes 24x7x365 log monitoring/correlation/alerting for these devices.

COOK COUNTY will only be billed as devices are turned up live.

5.3 MSS: Device Management

Cook County will be provided with 24x7 management support for the technologies in scope of Device Management, after in-scope devices have been implemented and pass Quality Assurance checks. For any other technology(s) brought into the Cook County environment that is out of scope and supported by SecureWorks, SecureWorks will address case by case. For REPLACEMENT of technology (switching out IPS/IDS or Firewall, for example) SecureWorks will continue to aid in implementation of those such devices. SecureWorks will notify Customer of any devices that are not supported prior to implementation.

5.3.1 Managed Advanced Malware Protection

SecureWorks will provide real-time management and monitoring of Advance Malware Protection appliances within scope, security event analysis and response for any Advanced Malware events 24 hours a day, 7 days a week, 365 days a year. SecureWorks Security Monitoring service combines our advanced Counter Threat Platform with a team of security analysts to deliver strong security and compliance value to our customers; per Exhibit E (Managed and Monitored Advanced Malware Protection). SecureWorks is providing Cook County the Silver tier of Advanced Malware Protection & Detection. Cook County is also subscribing to the CTU Custom Malware Analysis for 5/hours a month for the year – this service would take the place of the Gold tier and can be applied to all technologies, not just FireEye technologies.

COOK COUNTY will only be billed as devices are turned up live.

5.3.2 Managed Web Application Firewall

SecureWorks will provide real-time management and monitoring of Web Application Firewall appliances within scope, security event analysis and response for any Advanced Malware events 24 hours a day, 7 days a week, 365 days a year. SecureWorks will deploy, manage, and monitor Customer's web application firewall Devices. Deployment will consist of project management, solution design, and provisioning. Management will consist of establishing a baseline policy, tuning rules, executing change requests, reviewing signatures, and updating software. Monitoring will consist of health and security event analysis and response for the service level purchased per Exhibit E (Managed Web Application Firewall Service Description). Reports and ticketing will be available through the Portal.

COOK COUNTY will only be billed as devices are turned up live.

The fees for Year One Device Management and Monitoring include the following:

5.3.3 Managed and Monitored Standalone Physical Intrusion Detection/Prevention (IDS/IPS)

SecureWorks will provide real-time management and monitoring of IDS/IPS appliances within scope, security event analysis and response for events 24 hours a day, 7 days a week, 365 days a year. Pricing for IDS/IPS Monitoring, described below, is based on unit prices for in-scope quantities of Standalone IDS Devices monitored by SecureWorks. A "Standalone Physical IDS/IPS" is defined as a physical (non-virtual) device that only acts as an IDS/IPS. Pricing below includes any Monitored Standalone and/or Disaster Recovery (DR) "Standalone Physical IDS/IPS" rated at up to 40 gigabits per second (Gbps) throughput by the manufacturer. Any High Availability (HA) Physical IDS/IPS pair must be quoted separately. All devices must be on the SecureWorks supported Monitored IDS/IPS list and located within supported global geographies. Excludes any [REDACTED] IDS/IPS devices which can be quoted separately. Excludes any Host or Server IPS/IDS which can be quoted separately. Excludes management of any "Standalone Physical IDS/IPS" devices - only includes 24x7x365 log monitoring/correlation/alerting for these devices.

COOK COUNTY will only be billed as devices are turned up live.

The fees for Year One Standalone IDS/IPS Managed and Monitored with Console includes the following:

5.4 MSS: Implementation Fees

One-time MSS implementation fees are calculated as 1/12th of the total annual fee for services added to be billed for year one only of in-scope devices. If during the term of the Agreement COOK COUNTY increments the quantity of devices to be monitored for any given Service (MSS), the implementation fee charged will be 1/12th of the delta between the annual fee for the current range and the annual fee for the newly selected range, per Service.

Devices currently in scope but not yet activated will not incur any MSS implementation fee.

The MSS implementation fee shall be [REDACTED] and shall not exceed annual price of additional item. The MSS implementation fee shall only be incurred when Cook County activates more than 5 devices in a given quarter.

SecureWorks will provide real-time management and monitoring of CTA and Log Collectors appliances within scope, security event analysis and response for events 24 hours a day, 7 days a week, 365 days a year. The fees for the subscription of required (as currently scoped) SecureWorks hardware for MSS enablement, as described below shall be as follows:

[illegible]

The fee for the Advanced Threat Intelligence subscription service, as described in Exhibit D, shall be \$10,000/month. The fee for the Threat Intelligence Add-on: CTU Support & Custom Malware Analysis (5 hours/month) shall be \$5,000/month.

[illegible]

The fee for the Client Transition Services, as described in Exhibit A, shall be.
The fee for seven weeks of MSS Integration Plus, as described in Exhibit B, shall be.

[illegible]

The fee for the SDE is included in the overall cost of the contract. Any additional requests that are out of scope will be added by an additional cost and SOW.

Total Fees for Incident Management Retained Services:

other appropriate form of transportation within [REDACTED] hours for in-transit response supported location travel after the mutual determination by Customer and IR personnel that onsite IR is required.

Customer acknowledges and agrees that it is impossible and unrealistic for SecureWorks to anticipate every contingency in connection with emergency on site IR and, notwithstanding its commercially reasonable efforts, that there may be unforeseen circumstances or contingencies outside the reasonable control of SecureWorks that could make compliance with the foregoing unrealistic or impossible, regardless of cost, including but not limited to: holidays, acts of war or terrorism, weather, flight availability, visa and passport requirements, restrictions of importation of encrypted technologies, handler schedules, unanticipated levels of contemporaneous emergency incident responses and other similar or dissimilar circumstances or events.

5.9.1.4 Service Scheduling and Services Hold Terms

Once the Service Order Term has entered the final quarter or has expired, SecureWorks will implement the following restrictions on services. SecureWorks has no obligation to provide Services beyond the Services Term.

5.9.1.4.1 60 Days Prior to Services Term Expiration

[REDACTED]

- Compromise screening assessment services
- Incident management risk assessment services
- Incident response plan and playbook development services
- Incident response plan and playbook review services
- Incident response tabletop exercises services
- Incident response functional exercises services
- Incident response training workshop services
- Incident management workshop services
- Incident management briefings and advisory services

5.9.1.5 At Services Term Expiration

No proactive IR services will be available to the Customer.

5.9.2 Customer Obligations

Customer acknowledges that SecureWorks' ability to perform the Services hereunder is contingent upon the following:

- Customer resources are scheduled and available.
- For onsite Services to be performed, Customer has provided suitable workspace and necessary accesses for SecureWorks' staff and equipment.
- Access to Customer computer systems, devices and network as necessary to perform the Services is made available to SecureWorks.
- Replies to all document requests and other information are timely and in accordance with the delivery dates established in the planning phase.
- Customer scheduled downtime allows adequate time for SecureWorks' performance of the Services.

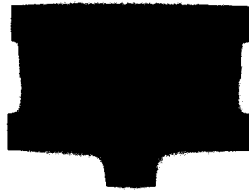
- Customer accepts responsibility for obtaining any and all necessary third party authorizations required to perform services in cloud, hosted, co-location or other environments not owned by Customer.

[illegible][illegible]

5.11 Total Costs

Advanced Security Services	Description	Quantity	Year 1	Year 2	Year 3
Dell SecureWorks - MSSP					
24x7 Monitoring Only:	Servers + Firewalls				
24x7 Managed & Monitored	IPS, IPS Console, [REDACTED]				
SecureWorks Required Analysis Tools & Log Collection		9			
Threat Intelligence	Advanced				
Optional Add-On	CTU MONTHLY SUPPORT HOURS	optional add-on			
Incident Management Services	Proactive & Reactive Incident Management Services	80 Hrs			
Minimum of 40 Hours per year, 80 Proposed					
Alerting & Reporting		included			
Training		included			
Total SecureWorks MSS					
Advanced Security Services	Description	Quantity	Year 1	Year 2	Year 3
Ascent Innovations - M/WBE					
24x7 Monitoring, No Management	[REDACTED]				
24x7 Monitoring, Only After Hours Management	[REDACTED]				

24x7 Monitoring, 24x7
Management



[Redacted] [Redacted] [Redacted]

Optional, 24x7
Monitoring, Only After
Hours Management

[Redacted]

[Redacted] [Redacted] [Redacted]

Optional, 24x7
Monitoring, 24x7
Management

[Redacted]

[Redacted] [Redacted] [Redacted]

Total Ascent MSS	[Redacted]	[Redacted]	[Redacted]

**Ascent Innovations -
M/WBE**

One-Time Implementation
& Project Management
Cost

[Redacted]

**Dell SecureWorks -
MSSP**

One-Time Project
Management

[Redacted]

Implementation, Integration, & Performance Tuning
and Optimization

[Redacted]

optional -
[Redacted]
weekly
increments
available

optional -
[Redacted]
weekly
increments
available

One-Time MSS Activation

[Redacted]

**Total for One-Time
Costs + Yearly
Performance Tuning**

\$184,500.00

**Total For all MSS
Services**

\$726,377.50

\$726,377.50

\$726,377.50

All Costs year 1

\$910,877.50

5.12 MSS Ordering

Customer acknowledges that an additional Service Order (SO) will be signed for any Managed Security Services (does not apply to Professional Services) delivered to COOK COUNTY not listed within this SOW.

5.13 Billing

Invoices:

100% billable within 45 days

Monthly Billing:

SecureWorks shall send Customer monthly invoices for the first month of the MSS Services, the full amount of Incident Management Retained Service, General Security Services and any other one-time MSS Service fees/Third-Party Purchase fees, upon the Service Commencement Date of the applicable MSS Service(s).

Thereafter, SecureWorks shall send monthly invoices to Customer for all MSS services and Resident services, including any professional services performed during the last month, during the remaining term of this SOW.

Billing Terms for Incident Management Retained Services:

- Service Fees for Year 1 are billable upon the commencement of the SOW Term.
- Service Fees for Year 2 are billable at the beginning of Year 2 after the commencement of the SOW Term or upon exhaustion of all previous Retained Hours.
- Service Fees for Year 3 are billable at the beginning of Year 3 after the commencement of the SOW Term or upon exhaustion of all previous Retained Hours.
- Retained Hours will be tracked in quarter hour increments.
- SecureWorks will keep Customer informed of the balance of Customer Retained Hours.
- Premium Incident Management Services may be required and added as needed, with Customer approval. Retained hours may be applied to Premium Services based on a factor of hours for every hour worked to the nearest half hour increment [REDACTED]
Premium Incident Management Services include:
 - Advanced Malware Analysis and Reverse Engineering Services
 - Incident Surveillance Services
 - [REDACTED] Targeted Threat Hunting and Response [REDACTED]
- Any distinction, variation, or designation of work that will be categorized as a "Premium Service" will be mutually understood and agreed upon before assignment or work is performed
- A fee of [REDACTED] per endpoint applies in addition to Service Fees should SecureWorks and Customer agree that malware detection and analysis on endpoint devices be applicable.
- Includes hours spent on delivering work, reporting, project management and all other work performed in this Engagement. Customer will not be invoiced for time spent traveling to an onsite response supported location.
- Reasonable out of pocket expenses for dedicated hardware, software and shipping costs as necessary for the Engagement as well as travel, food and lodging will be invoiced separately at actual costs. Travel will not occur without CISO approval and will follow Cook County travel policy.
- The determination of whether SecureWorks IR personnel are used for an incident will be made jointly by Customer and IR personnel during the initial contact call before any IR Services work effort is initiated.
- For each Year of the Term, available Retained Hours over [REDACTED] expire after [REDACTED] or upon expiration of SOW Term. Unused Retained Hours over [REDACTED] will be forfeited in each Year of the Term.

- Retained Hours expire after [REDACTED]. Any unused Retained Hours will be forfeited if unused within [REDACTED]. If the SOW Term is extended beyond [REDACTED], additional blocks of hours will need to be purchased at the time of the extension. On a case by case basis, SecureWorks will make commercially reasonable efforts to utilize available Retained Hours for other SecureWorks services, except those listed in this SOW.
- Additional Retained Hours must be acquired prior to the exhaustion of the Retained Hours balance for the response time commitment to remain in effect.
- This is a fixed work effort contract; not a fixed price contract. Additional blocks of hours may be retained in advance of exhaustion of contracted hours at the contracted rate above by the parties by executing a change order or an additional statement of work for such additional hours.
- Customer may authorize continued work effort for active cyber incident response services beyond the committed hours in 40-hour increments, via email to, to ensure continuous delivery of services. Additional hours must be authorized prior to the exhaustion of existing hours. Customer will only be billed for actual accrued hours.
- Customer will be invoiced immediately for committed hours and monthly for additional work activity against this SOW that are authorized via email.
- SecureWorks reserves the right to bill any cyber incident declared within fourteen (14) calendar days from the SOW Effective Date at the current Emergency Cyber Incident Response Services rate of [REDACTED] per hour.

5.14 Out-of-Pocket Expenses

The following out-of-pocket expenses are NOT included in the MSS Service fees: those related to transportation, meals and lodging to travel to perform the MSS Services. Customer agrees to reimburse SecureWorks for all reasonable and actual out-of-pocket expenses incurred for travel to the Customer location in the performance of the following Services hereunder. All travel will be required to be explicitly approved in writing by the CISO of Cook County.

Travel Expense Not to Exceed Amounts([REDACTED]/week)

- CTS - 4 one week trips - [REDACTED]
- MSS - 6 one week trips - [REDACTED]
- Cyber Security Incident Response Plan - 2 one week trips - [REDACTED]
- Incident Management Playbook Review - 2 one week trips - [REDACTED]
- Incident Management Table Top Exercises - 2 one week trips - [REDACTED]

Customer acknowledges and agrees that IR by SecureWorks requiring last minute air transportation will result in much higher and unpredictable costs than ordinary business travel as a result of the requirement to purchase tickets with little, if any, advance notice. Forensic work MAY also require additional costs associated with required media storage, specific equipment or licensing, depending on the size of the incident, image acquisition needs or the complexity of the incident. Such expenses will be added, at cost, to Customer's invoice.

6 Customer Obligations

Customer acknowledges that SecureWorks' ability to perform the MSS Services hereunder is contingent upon the customer requirements listed in the attached service descriptions, Exhibit C through J, and upon the following:

- Customer resources are scheduled and available during a mutually agreed schedule.
- Customer installs all customer premise equipment (CPE) as stated in SD/SLA documents.

- For onsite Services to be performed, Customer has provided suitable workspace and necessary accesses for SecureWorks' staff and equipment.
- Access to Customer's computer systems, devices and network as necessary to perform the Services is made available to SecureWorks.
- Replies to all document requests and other information are timely and in accordance with the delivery dates established in the planning phase.
- Customer scheduled downtime or testing windows allow adequate time for SecureWorks' performance of the Services.
- Customer's contracted third parties involved in an Engagement will be cooperative and forthcoming with required information. Such cooperation includes but is not limited to the following:
 - Actions taken during the course of the investigation
 - Findings reports from any other investigative firms
 - Providing SecureWorks copies of original evidence files and or images where sound forensic processes were employed
- Customer acknowledges that they are the best informed as to their contractual privileges and responsibilities with respect to contracted third party services such as Cloud or hosted environments and will provide SecureWorks with authoritative positions regarding permissions to operate in third party environments for the purposes of this SOW.
- Customer accepts responsibility for obtaining any and all necessary third party authorizations required to perform services in Cloud, Hosted, Co-location or other environments not owned by Customer.

7 Term

SOW Term:

The term of this SOW shall commence on the PSA Effective Date and terminate on the earlier to occur of (i) the date which is three (3) years thereafter, or (ii) the completion of the Services (the "SOW Term").

The term of the Services for the Incident Management Retainer shall commence on the PSA Effective Date and terminate on the earlier to occur of (i) the SOW term, or (ii) upon exhaustion of the original Retained Hours (or subsequent change order) and completion of any outstanding time and materials billing (the "Services Term").

To the extent that Customer authorizes continued work effort for active cyber incident response services pursuant to Section 5.2 above, and such continued work effort extends beyond the PSA Term and/or Services Term, the SOW Term and Services Term may be extended to the completion of such continued work effort (the "Extended Term"). During such Extended Term, the terms and conditions of this SOW and the MSA shall be in full force and effect.

Upon completion of the Services, the Customer designated contact will receive an email confirmation from SecureWorks. Unless otherwise notified in writing to the contrary by the Customer designated contact within thirty (30) days of such email confirmation, the Services and this SOW shall be deemed complete.

MSS Services Term: The term of the MSS Services shall commence on the Service Commencement Date and will terminate three years from the Service Commencement Date, if not otherwise earlier terminated in accordance with the provisions of the MSA and/or this SOW ("Services Term"). Thereafter it may be renewed by customer for an additional two (2) terms of one (1) year each

("Renewal Term(s)") at Customer's sole discretion. The price will be fixed for the Service Term, and may increase by the lesser of CPI or three (3) percent for any Renewal Term.

8 Other Terms

- A) The parties acknowledge and agree that: (a) the terms and conditions of this SOW are incorporated in the PSA herein by reference; (b) this SOW will be deemed an addendum to and part of the PSA; (c) in the event of any conflict or discrepancy between the terms or provisions of the PSA and this SOW, the terms and provisions of this SOW shall control and govern (but only for the purpose of this SOW); and (d) except as set forth herein the terms and conditions of the PSA shall remain in full force and effect and are hereby ratified and reaffirmed.
- B) SecureWorks provides Customers with expert and timely security analysis. However, deployment of SecureWorks' MSS Services in a Customer network does not achieve the impossible goal of risk elimination, and therefore SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on a Customer network.

SecureWorks may schedule maintenance outages for SecureWorks-owned Equipment/servers which are being utilized to perform the MSS Services with twenty-four (24) hours' notice to designated Customer contacts. SecureWorks works with the client to ensure schedule is acceptable.

- C) The Service Levels inherent set forth herein are subject to the following terms, conditions, and limitations:
 - i) The Service Levels shall not apply during scheduled maintenance outages and therefore are not eligible for any Service Level credit during these periods.
 - ii) The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits SecureWorks from providing the MSS Service, delivering the Service Levels or managed service descriptions, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the MSS Services, or any unauthorized modifications made to any managed hardware or software devices by the Customer, its employees, agents, or third parties acting on behalf of Customer.
 - iii) Furthermore, the Service Levels shall not apply to the extent Customer does not fulfill and comply with its obligations set forth within this SLA. The obligations of SecureWorks to comply with the Service Levels with respect to any incident response or help desk request are conditioned upon SecureWorks' ability to connect directly to the Customer devices on the customer network through an authenticated server in the SecureWorks Secure Operations Center.
- D) Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to SecureWorks of such failure. Service Credits are calculated according to the impacted MSS Services, not the entire monthly bill. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to SecureWorks within thirty (30) days of such Service Level failure. SecureWorks will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to Customer in connection with any of the above Service Levels failures in any calendar month will not exceed the monthly MSS Service fees paid by the Customer MSS Service(s). In cases in which only one or some of a Customers' devices were impacted, MSS Service credits will be further pro-rated to only apply to the impacted Customer devices. In the event of SecureWorks' default, Service Level credits issued pursuant to this Section do not preclude the County from seeking all remedies available under the Professional Services Agreement.
- E) SecureWorks will troubleshoot and, if necessary, replace any Log Retention Appliances in accordance with the terms for iDevices provided in on page 8 of Exhibit C -SecureWorks Maintenance Program Terms and Conditions.

- F) In the event that Customer data contained on the Log Retention Appliance exceeds the appliance's storage or processing capacity, Customer has the option to purchase one or more additional Log Retention Appliances to accommodate the increase in customer data. The SLAs shall not apply in the event of MSS Service interruption due to lack of storage space on the Log Retention Appliance.
- G) Disclaimers
- i) Applicable to Onsite Services: Notwithstanding employees' placement at the Customer location, SecureWorks retains the right to control the work of the employee. For international travel, Onsite Services may require additional documentation, such as Visas, visitor invitations, etc. which may affect timing and out of pocket costs.
 - ii) to Security Services: Should a Statement of Work include security scanning, testing, assessment, forensics, or remediation Services ("Security Services"), Customer understands that SecureWorks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. Customer authorizes SecureWorks to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services or otherwise approved by Customer from time to time) on network resources with the IP Addresses identified by Customer. Customer represents that, if Customer does not own such network resources, it will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to SecureWorks, to permit SecureWorks to provide the Security Services. SecureWorks shall perform Security Services during a timeframe mutually agreed upon with Customer. The Security Services, such as penetration testing or vulnerability assessments, may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom coded applications but will exclude intentional and deliberate Denial of Service Attacks. Furthermore, Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the Customer's systems and accepts those risks and consequences. Customer hereby consents and authorizes SecureWorks to provide any or all the Security Services with respect to the Customer's systems. Customer further acknowledges it is the Customer's responsibility to restore network computer systems to a secure configuration after SecureWorks' testing.
- H) Applicable to Compliance Services: Should a Statement of Work include compliance testing or assessment or other similar compliance advisory Services ("Compliance Services"), Customer understands that, although SecureWorks' Compliance Services may discuss or relate to legal issues, SecureWorks does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by SecureWorks in connection with any Compliance Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer's legal or regulatory compliance.
- I) Applicable to PCI Compliance Services: Should a Statement of Work include PCI compliance auditing, testing or assessment or other similar PCI compliance advisory Consulting Services ("PCI Compliance Services"), Customer understands that SecureWorks' PCI Compliance Services do not constitute any guarantee or assurance that security of Customer's systems, networks and assets cannot be breached or are not at risk. These Services are an assessment, as of a particular date, of whether Customer's systems, networks and assets, and any compensating controls meet the applicable PCI standards. Mere compliance with PCI standards may not be sufficient to eliminate all risks of a security breach of Customer's systems, networks and assets. Furthermore, SecureWorks is not responsible for updating its reports and assessments, or enquiring as to the occurrence or absence of such, in light of subsequent changes to Customer's systems, networks and assets after the date of SecureWorks' final report, absent a signed Statement of Work expressly requiring the same.
- J) Record Retention

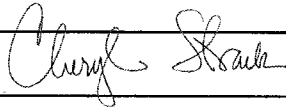
- i) SecureWorks will retain a copy of the Customer Reports and supporting Customer Data in accordance with SecureWorks' record retention policy, which provides such retention for a period commensurate with such Customer Reports and supporting Customer Data usefulness and SecureWorks' legal and regulatory requirements and SecureWorks' directives.
 - ii) Unless Customer gives SecureWorks written notice to the contrary prior thereto, then thirty (30) days after delivery of its final report, SecureWorks shall have the right, in its sole discretion, to dispose of all acquired hard drive images and other report backup information acquired in connection with its performance of its obligations under this SOW.
- K) Post Engagement Activities

Upon the "Engagement Conclusion" defined as the earlier to occur of (i) acceptance by Customer of the final Customer Report, or (ii) thirty (30) days after the delivery of the final Customer Report, SecureWorks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by SecureWorks in the performance of the Services hereunder (the "Incident Media"), unless prior to such commencement, Customer has specified in writing to SecureWorks any special requirements for SecureWorks to return such Incident Media (at Customer's sole expense). Upon Customer's request, SecureWorks will provide options for the transfer to Customer of Incident Media and the related costs thereto. If so requested, SecureWorks will provide a confirmation letter to Customer addressing completion and scope of these post incident activities, in SecureWorks' standard form. Unless agreed to otherwise by, SecureWorks shall, in its sole discretion, dispose of the Incident Media on or after the Engagement conclusion and only maintain a copy of the final Customer Report and associated deliverables.
- L) Legal Proceedings

If Customer knows or has reason to believe that SecureWorks or its employees performing Services under this SOW have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require SecureWorks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify SecureWorks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse SecureWorks for (a) its employees' time spent as to such response at the hourly rate reflected in this SOW, (b) its reasonable and actual attorney's fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and SecureWorks as to the Services or this SOW.
- M) Endpoint Assessment - Malware Hunting

Unless otherwise agreed upon in writing, within sixty (60) days following the expiration or termination of this SOW (the "Thirty Day Period"), Customer shall uninstall any and all copies of the software agent used for Malware Hunting. During the sixty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install SecureWorks' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of SecureWorks from the software agent. Customer will uninstall the software agent as described in this SOW.

By their signature below, SecureWorks and Cook County Government indicate their agreement to the terms and conditions set forth in this Agreement.

SecureWorks, Inc.	
Signature:	
Name:	Cheryl Strack
Position:	Contracts Senior Advisor
Date:	7/8/2016

Cook County Government	
Signature:	
Name:	
Position:	
Date:	

CERTIFICATE OF INCUMBENCY

I, George Hanna, Vice President and General Counsel of SecureWorks, Inc. (the "Firm"), a company duly organized and validly existing under the laws of the state of Georgia, hereby certify as follows:

I have reviewed the constitutional documents and resolutions of the Board of Directors of SecureWorks Corp., a Delaware corporation, of which the Firm is a wholly-owned subsidiary, and certify that the individual named below is authorized to act on behalf of the Firm to sign, execute and deliver, on behalf of the Firm, the Economic Disclosure Statement and Identification of Subcontractor/Supplier/Sub-consultant Form with The County of Cook located in Chicago, IL. The person named below is duly qualified and acting representative of the Firm, duly appointed and authorized to sign the Economic Disclosure Statement and the Identification of Subcontractor/Supplier/Sub-consultant Form aforementioned and all documentation required by The County of Cook located in Chicago, IL for this purpose. The signature set opposite the name of that person is the genuine signature of said person.

Name

Cheryl Strack

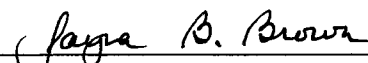
Signature



George Hanna, Vice President and General Counsel of
SecureWorks, Inc.

State of Georgia
County of Cobb

Signed and sworn to before me on this 22nd day of July, 2016, by George Hanna, Vice President and General Counsel of SecureWorks, Inc., a company duly organized and validly existing under the laws of the state of Georgia, who is personally known and/or proved to me on the basis of satisfactory evidence, to be the person who appeared before me.


Notary Public

My Commission Expires:

3/20/2018

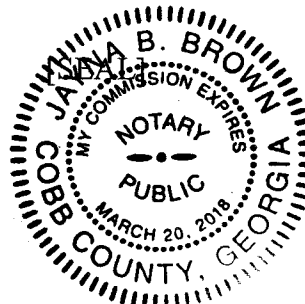


Exhibit A - Customer Transition Services

Customer Transition Services Methodology

SecureWorks understands that transition can be the most challenging part of any IT outsourcing engagement and assumes mission-critical significance. Our goal is to achieve program success through consistent planning, execution, and governance and to ensure the successful delivery of complex service transition in a predictable and organized manner. The objectives that inform our achievement of our goal are:

- Optimize transition between functions
- Central management of change (risk/action/issue/decision)
- Establish accountability (plan/run/govern)
- Manage competing priorities (balance)
- Facilitate communications (visibility)
- Accelerate time to value

Our methodology is built on accountability, balance and communication that provides a structure transition which:

- Establishes accountability across delivery resources with a foundation in collaborative planning
- Maintains balance in execution by governing delivery, capacity and priorities
- Leads communication across stakeholder groups to keep everyone informed and aligned

The high level components of our transition method are planning, execution and governance.

Planning

Transition starts when SecureWorks schedules a soft launch conference call with Customer to conduct introductions, discuss the transition methodology and associated processes, agree on next steps, and set a date and time for a detail planning session at one of Customer's facilities.

The planning sessions goal is to produce a schedule of activities aligned within milestones and inclusive of dates, accountability for each activity, as well as setting up the transition governance committee and establishing the cadence for ongoing transition governance calls to review progress and manage exceptions through RAID alignment and management.

Planning Work Session

The planning work session will take the output from the soft launch which includes a scope review, identification of deliverables and dependencies and an outline of a draft schedule. The comprehensive review of the scope, deliverables, dependencies, risks, and stakeholders and the initial planning session is the foundation for successful execution of the transition.

Execution

Managing and maintaining the schedule and RAID log, as well as balancing priorities across all functions are the focus of the execution process. The transition program manager handles delivery, manages capacity, and keeps priorities aligned. The integration and cycles of progress reviews and exception management are key inputs to execution activities which include:

- Maintaining the schedule
- Maintaining the RAID log
- Monitoring delivery progress
- Monitoring scope, time, cost and quality

- Maintaining the balance of priorities

Ongoing review of risks and issues, assigning actions and making decisions, are vital components to staying on schedule and meeting the goals of a successful transition program.

Governance

The agreed upon communication plan is the core of the governance process. The transition governance committee, led by the transition program manager, will review progress to schedule and RAID on a weekly basis. The transition program manager also provides a weekly status for all stakeholders inclusive of executives and sponsors. The goal of ongoing transition program governance is to effectively manage each objective (time, cost, quality, benefits, risk, and scope).

The weekly status communicates issues, needs, and overall progress (completed and planned) collaboratively with the joint Customer and SecureWorks transition governance committee.

Transition Program Manager

The following information highlights the base role and responsibility as well as knowledge and skills we employ in a transition program manager position.

Role Responsibilities

- Manage expectations and provide executive level reporting
- Oversee program of complex projects driving service transition and onboarding
- Govern program of projects include driving schedule, cost, and scope
- Manage and mitigate risk, actions, issues and decisions on all projects
- Provide oversight and reporting to budget and contract milestones
- Develop program's key objectives, scope, success criteria and communicate them effectively across the program stakeholders
- Liaise across functions; interface with leadership and functional teams to provide transparency of project health
- Manage all aspects of complex program of projects for the respective lines of business from inception through delivery
- Define and review reports to ensure all services are completely and successfully delivered
- Proactively engage to correct problems when they are encountered.
- Work effectively with other IS teams and outsourcing provider(s) to ensure technology solutions are effectively managed and performed
- Implement best practices to increase customer satisfaction: meet professional services revenue and profit quotas while managing P&L; responsible for staff/account management, prioritization and forecasting; develop and maintain world-class processes and personnel; provide delivery management to ensure customer satisfaction

Minimum Knowledge and Skills Required

- 8+ years of demonstrable experience leading customer service transitions through complex cross functional program of projects
- Experience leading through thought leadership and vision, with a mind's eye to quality delivery and Customer first
- Experience reporting to and working with executive management
- Excellent communication and presentation skills
- Experience negotiating and managing stakeholder expectations
- Experience with financial responsibilities and strategy

- Experience managing a security program for large companies
- Solid understanding of risk-based security strategies
- PMP desired
- CISSP CSM, CISA, GIAC, or other security certification desired

Deliverables

The Transition Service will be performed by one or more expert transition program managers with extensive experience managing security services transitions assigned from SecureWorks' Global Transition Management and Customer Success (GTM&CS) team. The transition program manager will seek to quickly understand the workings of Customer's environment with respect to their requested services in order to optimize transition of the Security Services(s). The transition program manager maintains key relationships with each of SecureWorks service towers leaders and their resources which are instrumental to plan, execute, and govern transition of security service(s).

The contracted transition services are based upon the complexity and maturity of Customer's security environment, and the contracted scope and scale of the security service(s) particular to the implementation. The transition service components will be performed remotely by the transition program manager. It is common for an initial detail planning session onsite at one of Customer's facilities, as appropriate and agreed upon by the parties.

The transition program manager will schedule a soft launch kickoff call with Customer to conduct introduction and discuss timeline, governance, resources/stakeholders and high-level objectives. During this initial call, the parties will discuss any documentation supplied, define rules of engagement, and ensure that the scope and expectations for the Service(s) are clearly identified and defined. The high level transition management deliverables include:

- Program schedule
- RAID Log (risk, action, issue, decisions)
- Stakeholder roles and responsibilities (RACI)
- Communication plan
- Scope, time, cost, quality management plan
- Weekly consolidated executive status
- Lessons learned

COOK COUNTY Specific Deliverables

- All deliverables listed under managed security services (MSS), endpoint services and threat intelligence are considered upfront deliverables. This implies that these services have been deemed critical to the onboarding process and must be completed as part of the initial deployment.
- Services such as vulnerability scanning and penetration testing will be delivered over time, however COOK COUNTY will require documentation and training to be provided as upfront deliverables.
- Incident response is broken down into two distinct parts, proactive and reactive. SecureWorks will provide COOK COUNTY with reasonable estimates of the necessary hours needed deliver the services requested. SecureWorks will also ensure that these estimates are properly accounted for in the statement of work.

Managed Security Services (MSS)

- SecureWorks will provide validation that all data being collected from in-scope devices is in the proper format and is being processed correctly.
- SecureWorks will provide validation that any physical or virtual appliance purchased by COOK COUNTY is properly installed, configured, sized and tuned appropriately.

- SecureWorks will provide validation that any data collected from COOK COUNTY is being stored, processed or transmitted securely.
- SecureWorks will provide documentation which details access controls and permissions to any device that stores, processes or transmits COOK COUNTY data.
- COOK COUNTY will develop and execute a plan to test the resiliency of any physical or virtual appliances purchased from SecureWorks for the delivery of the Services listed in this SOW are implemented in a way that fits our enterprise security architecture and network requirements.
- At the end of the deployment period, SecureWorks will provide a report to COOK COUNTY in order to show that all MSS services have been implemented as agreed.
- SecureWorks will provide documentation to show that all devices in-scope for MSS have been successfully on boarded.

Endpoint Services

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Threat Intelligence

SecureWorks will provide documentation to show that all threat intelligence services have been configured and activated successfully.

- Enterprise brand surveillance
- Enterprise threat intelligence
- Borderless threat management profile
- CTU countermeasures
- Attacker Database

Training

SecureWorks will provide COOK COUNTY with access to the SecureWorks University training portal.

In addition, the training initiatives SecureWorks will also provide the following

- Development of a training program for the purposes of knowledge transfer to ISO Cook County staff upon notification of termination of services contract.
- Development of a project timeline identifying training, delivery dates, and resources
- Development of training criteria including creation of standard operating procedures

Integration

SecureWorks will provide documentation showing how their services have been integrated with COOK COUNTY systems.

Miscellaneous

- SecureWorks will provide portal training to COOK COUNTY
- SecureWorks will provide documentation for any and all processes by which COOK COUNTY support teams would engage the SecureWorks SOC.
- SecureWorks and COOK COUNTY will develop escalation processes, paths and contacts relating to the incident handling process.
- COOK COUNTY and SecureWorks will review the SIF and ensure that the document contains all relevant systems which are considered in-scope for the engagement.
- SecureWorks will provide documentation for all SLAs included in-scope for the engagement.
- SecureWorks will work with COOK COUNTY to create meaningful metrics and reporting regarding service delivery and performance.

Transition Initiation

The transition program manager will be assigned in advance of the scheduled start date and request documentation from Customer in order to review current processes, personnel, and data, in order to become familiar with Customer's organizational structure, personnel, business environment, and current security program. The transition program manager will meet with Customer early and advise on next steps that reflect Customer's unique needs, requirements, and expectations. Customer will interface with other internal stakeholders and SecureWorks for scoping and scheduling of the program. The transition program manager will develop an initial program schedule and RAID log and conduct a kick-off call with Customer to facilitate introductions, discuss high level scope and resources, and to schedule the onsite planning work session. Initial activities include:

- Review SOW
- Review resources with SecureWorks delivery leads
- Review account with SecureWorks Sales Account Management
- Confirm scope, assumptions, and acceptance
- Confirm deliverables and dependencies
- Confirm timeline, constraints, prerequisites
- Confirm Customer resources (technical, Project Management Office (PMO))

Transition Planning

Transition planning focuses scoping, resourcing, tasking, dependencies, constraints, and roles and responsibilities while managing the overall objectives of time, cost, quality, benefits, risk, and scope. An onsite planning session is conducted to:

- Initialize Schedule
- Initialize Risk, Action, Issue, and Decision Log
- Finalize Stakeholder Roles and Responsibilities
- Finalize Communication Plan
- Initialize Scope, Time, Cost, and Quality Management

- Align with Customer governance

Planning Activities

- 1) Sales or account manager notifies Transition Manager of new SOW and all required groups review SOW
 - a) Scope
 - b) Dependencies
 - c) Required deliverables
- 2) Account manager, solution architect, transition manager and provisioning project manager conference with customer to do introductions discuss governance and set a date for the face-to-face program planning session
- 3) Service Area PMs or Technical Leads Prepare Task Plan based on SOW requirements
 - a) Provide key activities, dependencies and needs to transition manager
- 4) Transition manager prepares draft program schedule based on service area activities in the approved SOW
 - a) Leverage standard template with modifications specific to the SOW provided by Service Areas
- 5) Transition Manager conducts Customer facing planning session
 - a) Attendees include Customer sponsor, Customer PMO, Customer technical leads, SecureWorks Account Manager, SecureWorks Transition Manager, CIS Project Manager/Project Engineer
 - b) Optional attendees as defined in the soft launch could include managed security services integration (MSSi), security risk and consulting (SRC), residency
- 6) Transition manager finalizes schedule based on planning session
 - a) Includes updating the risk and issue log, stakeholder RACI, Communication Plan
 - b) Sets up weekly governance review
 - c) Notifies service areas to set up technical kickoff and review calls for deliverables

Transition Execution

Transition execution focuses on managing schedules, issues and priorities related to goals and ongoing progress while ensuring quality outcomes and mitigating risk.

- Manage delivery
 - Manage delivery against a jointly developed schedule
 - Manage and schedule resources
 - Communicate dependencies that impact timelines and resources
 - Escalate dependencies that impact delivery well before overruns are experienced
 - Prepare and agree mitigation plans with Customer to overcome delays and issues
 - Manage RAID (Risks, Action Items, Issues, and Decisions)
 - Capture lessons learned for review upon program completion
 - Align with Customer change processes
- Manage scope
 - Ensure project scope is delivered within the agreed time, cost, and quality
 - Raise and mutually agree on change requests on scope, time, cost or quality
 - Obtain weekly status reports from each stakeholders group in prep to roll up to overarching program status
 - Hold weekly status and or technical review calls with the assigned stakeholders

- Manage quality
 - Oversee the quality of technical deliverables through scheduled reviews, peer reviews, and Customer walkthroughs
 - Align with Customer quality review requirements

Execution Activities

- 1) Service area project managers or technical leads conduct technical calls as needed
 - a) Kickoff technical install (requirements confirmation, Service Installation Form (SIF) Intro, scope review, communicate information needed)
 - b) Periodic technical reviews (Review Information received, Review SIF, implementation work session)
 - c) Deliverable review (review draft and final deliverables, test, signoff)
- 2) Service area project managers or technical leads provide updates to Transition Manager
 - a) Progress on key activities outlined mapped to the program schedule
 - b) Communication needs and issues
- 3) Transition Manager consolidates all Service Area progress updates
 - a) Updates program schedule
 - b) Updates Executive with 4up reporting format including any needs/issues
 - c) Forwards schedule and 4up reports in advance of governance review
- 4) Transition Manager conducts weekly governance review walking through the Executive 4up and schedule updates
 - a) Attendees include Customer sponsor, Customer PMO, Customer technical leads, DSW Transition Manager, DSW Account Manager, CIS PM/PE
 - b) As needed attendees include MSSi, VMS, GRC, SRC, Residency where attendance depends on needs and issues identified by those groups.
- 5) Transition Manager updates risk, issue, action, and decision (RAID) log including any escalation or change processes
- 6) Transition Manager schedules and conducts any specific breakout discussions warranted based on the governance call, risks, issues, or changes.

Transition Governance

Transition governance focuses on achieving a structured approach to conducting transition tasks while minimizing the impact on the business-as-usual activities. Through the governance process and communication plan we will manage accountability in all areas of the program including delivery, capacity, priorities and stakeholder alignment.

- Review Progress
 - Review delivery progress against a jointly developed schedule
 - Review Stakeholder involvement against jointly developed plan
 - Review RAID log against tractable items
 - Escalate new risks or issues daily/weekly
 - Capture lessons learned for review upon program completion
- Manage Communications
 - Provide a consolidated executive status weekly
 - Provide an updated schedule weekly
 - Provide an updated RAID log weekly
 - Communicate change needs against scope, time, cost, or quality
 - Manage escalations keeping all parties regularly informed on progress and mitigation

- Provide internal SecureWorks Program Pulse Progress Update

Transition Closure

Transition closing focuses producing the final report to Customer, capturing lessons learn and turning the transitioned services over the steady state delivery team.

Conduct Program Close

- Prepare/review final executive report
- Review Lessons Learned captured during program
- Upload all Progress Reports, Documentation, written Deliverables, final Schedule, final RAID, and other Program Artifacts to Internal Transition Services repository
- Close any Time and Cost Accounting as needed
- Obtain final signoff as needed
- Complete turnover of transition to steady state services team and service delivery executive (SDE)

Exhibit B - MSS Integration Plus Service

MSSI+

Every Managed Security Services ("MSS") installation is unique, especially in complex technology environments. The MSS Integration Plus ("MSSI+") service (the "Service") is designed to assist Customer in better integrating their MSS Service(s) into their business processes in order to obtain maximum value from the contracted MSS Service(s). The Service will be performed by one or more expert security consultant(s) assigned from SecureWorks' Security and Risk Consulting ("SRC") team (each a "Security Consultant"), who will seek to quickly understand the intricacies of Customer's environment in order to optimize the integration and performance tuning of the MSS Service(s). Consultant is a subject matter expert ("SME") on all SecureWorks services and is part of a team dedicated to delivering Service.

The Service components to be performed (as set forth below) are based upon the complexity and maturity of Customer's security environment and the contracted MSS services which are unique to each Customer. During the Services Term (as defined below), Customer may select one or more Service components set forth below to be performed by SecureWorks. The Service components may be performed remotely from one of SecureWorks' facilities and/or onsite at one of Customer's facilities, as appropriate and agreed upon by the parties. The duration of the Service is agreed upon by the parties as set forth in the SOW (the "Service(s) Term").

The MSSI+ Service Term is a defined period of time of 7 weeks. The Security Consultant will use best efforts to accomplish as many MSSI+ Service components as possible during the Services Term; as such, components are determined by Customer. The Service components that can be delivered will depend upon where Customer is in their MSS implementation lifecycle and the contracted MSS services subscribed.

[REDACTED]

[REDACTED]

[REDACTED]

Exhibit C - Monitored Security Services



Monitoring Service
Description & SLA (9

Alerting & Reporting

SecureWorks will provide Cook County with 24 x 7 alerting and reporting of all ISO technologies within scope. Alerting and Reporting capabilities will include the following;

- Carrying out event analysis with the statistical events correlation rules. This should include the correlation of the events from all the devices within the on premise [REDACTED]
- Preparing daily/ weekly / monthly/yearly reports to summarize the list of incidents, security advisories, vulnerability management, and other security recommendations. It should include the operations trend analysis with the reports correlation of the present and past data
- Tracking impact of new vulnerabilities and threats on County's affected assets
- Tracking and supporting implementation and coordinate for closure of vulnerabilities on assets that are affected in mutually agreed upon formats
- Providing a security dashboard for an online view of the global vulnerabilities and threats applicable to the County's environment, number of assets affected and status of mitigation
- Providing an online secured portal for
 - real-time monitoring of analyst investigations
 - All incidents tracked and their history
 - Change requests
 - Running shift log containing detailed security analyst notes on investigations and other daily operations
 - Standard Operating Procedures
 - Run books
 - Quick reference guides
 - Secure document exchange
 - Reports
 - Email notification of new and modified tickets. Priority ticket notifications are also available to different email addresses[REDACTED]
- Customizable user interface
- Evaluating and prioritizing security alerts from ISO technologies.
- Creating relevant security alerts from ISO technologies.
- Providing Compliance-oriented reports for daily review
- Providing Security incident summary and details
- Providing Trend analyses that reveal trends in policy exceptions and user behavior
- Recommending events that should be categorized as "special attention"
- Analyzing Event source inventory and summary
- Creating Service level agreement metric reports
- Providing Incident identification and response services

- Providing trending reports on a monthly, quarterly and yearly basis
- Providing executive reports on an ad-hoc basis
- Assuring all service requests and help desk tickets are entered on County's Help Desk System or as mutually agreed upon
- Providing specific SIEM reports and alerts that are able to address the following use cases, but not limited to:
 - Botnet activity
 - Virus outbreaks
 - Unauthorized remote access
 - Suspicious activity (terminated account access, key loggers, international VPN access, etc.)
 - After hours badge access
 - Disabling system service accounts or services
- Assisting ISO in determining Key Performance Indicators (KPI) and information security metrics for tracking and reporting
- Maintaining proper inventory and network diagram of assets used in the ISO infrastructure

Exhibit D - Threat Intelligence Services



SD-SLA - CTU Threat
Intelligence - English

Exhibit E – Device Management Services



Managed and
Monitored Advanced



Managed Web
Application Firewall Se

Exhibit F – Incident Management Retained Services

Incident Management Response Services Pre-Planning and Coordination

Upon SecureWorks' receipt of this Customer executed SOW; SecureWorks will begin establishing workflows to support Customer requests for Incident Management Services. The following actions will be taken by SecureWorks personnel and are considered non-billable:

- Distribute contact information to Customer for engaging with SecureWorks for IR and digital forensics services. Contact information includes the 24/7/365 IR hotline, the IR Resource Coordinator and IR Delivery Managers;
- Provide Customer with artifact acquisition, chain of custody and secure transport instructions;
- Facilitate a Service initiation conference call with the Customer point of contact to review all Services available, clarify escalation channels and verify Customer contact information;
- Provision Customer access to the Portal for IR and forensics service request tickets;
- Coordinate Retained Hour utilization notifications and facilitate non-billable, on-demand meetings to scope proactive and reactive Service Engagements.

Retained Incident Management Services

Incident Management Briefings and Advisory

Upon SecureWorks' receipt of a Customer Authorized Engagement request, conference calls or onsite workshops can be arranged to review lessons learned from previous incidents that have occurred, to review the overall status of the Customer's Incident Management program, or provide guidance on topics of interest that fall within the domain of Incident Management.

Proactive Service Options

Incident Management Workshop

Upon SecureWorks' receipt of a Customer Authorized Engagement request, an onsite SecureWorks consultant ("Consultant") led workshop can be arranged during the Services initiation process to review IR capabilities with Customer key personnel and conduct a tabletop exercise to establish IR processes for engaging with SecureWorks for Incident Management Services. This optional workshop allows SecureWorks to become familiar with Customer's organizational risk profile, logging and detection capabilities, IR capabilities and key personnel prior to responding to any active IR support requests. This workshop will support the creation of an information profile on the Customer's environment for SecureWorks IR personnel to provide more efficient and tailored Services.

Incident Response Plan and Playbook Reviews

Upon SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks will conduct a detailed review of Customer's existing IR capabilities. SecureWorks will request documentation that supports the effort to understand the Customer's current IR posture and practices in order to provide an analysis of IR capabilities based on SecureWorks' breadth of experience, recommendations based on assessment of Customer's environment and relevant standards or regulatory requirements. The documentation requested will consist of items such as process diagrams, policies, procedures, guidelines and any other pertinent information to help SecureWorks understand Customer's current practices and regulatory requirements. As deemed necessary, facilitated workshops and interviews may also be conducted with Customer key stakeholders to rapidly gather a deeper understanding of overall requirements, critical business requirements and existing response capabilities. It is anticipated that Customer's Engagement point of contact will provide the requested information and access to key

stakeholders as rapidly as possible once the Engagement begins. At the close of the Engagement, Customer will receive a risk prioritized findings and recommendations report to improve IR practices.

Incident Response Training Workshops and Exercises

Upon, SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks will facilitate IR Training Workshops with specific topics customized to improve Customer's IR capabilities. SecureWorks will also test Customer's IR plan with facilitated tabletop and functional exercises. SecureWorks testing exercises feature tailored threat scenarios relevant to Customer's organization that are intended to proactively highlight gaps or issues with Customer's strategies and plans.

Incident Response Training Workshops

The content covered in IR Training Workshops will vary based on the maturity of existing capabilities and desired objectives. Available IR Training Workshop options may include:

- IR Fundamentals
- Evidence Handling and Chain of Custody
- Volatile Data Collection and Analysis
- Forensic Imaging Techniques
- Basic Forensic Analysis
- Malware Analysis for First Responders

Incident Response Tabletop Exercises

An IR tabletop exercise involves assembling key IR stakeholders in a single place and walking through a scripted exercise. The facilitator releases information concerning the incident in a controlled manner that will guide the exercise, while each stakeholder describes the role they would play in a real incident. IR tabletop exercises are an efficient way to familiarize staff with IR practices and proactively test existing response plans. IR tabletop exercises are highly effective to validate roles, responsibilities, coordination and decision-making.

Incident Response Functional Exercises

Functional exercises are appropriate after tabletop IR exercises have already been performed and lessons learned from previous tabletop IR exercises have already been adopted. Functional exercises allow Customer's personnel to validate their operational readiness for incidents by performing their duties in a simulated manner. Functional exercises are designed to exercise the roles and responsibilities of specific team members and procedures in one or more functional aspects of a plan. Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. SecureWorks can coordinate overt and covert IR functional exercises.

An **overt functional exercise** involves the participants functionally performing each step of the plan as if it were a real incident. All participants are aware that it is an exercise, but attempt to perform actual response activities during the exercise.

A **covert functional exercise** is where only the Engagement point of contact or their designee is aware that the testing is an exercise. Typically, only organizations that have mature response capabilities undertake covert functional exercises due to the complexity of preparing and coordinating this type of response exercise.

IR training and exercise Engagements include the following major delivery phases:

- One Consultant will review existing IR materials and work with the Customer Engagement point of contact to verify the overall test plan and scenario injects are appropriate;
- At least one Consultant will be scheduled for one day onsite to function as the facilitator and data collector for the exercise. For exercise groups larger than ten people, for exercises that

span multiple locations, or for any functional exercises, the facilitator and data collector roles will require at least two Consultants;

- One Consultant will provide Engagement after action reporting and follow-up support.

At the close of a training or response exercise Engagement, Customer will receive an after action report that summarizes the event activities with risk prioritized findings and recommendations to improve IR practices.

Incident Response Plan and Playbook Development

Upon SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks will assist with developing IR Plan materials at both a strategic and tactical level. At the strategic level, SecureWorks will assist with IR plan development, security policy integration, capability development and governance. From a tactical standpoint, SecureWorks will help define IR workflows, roles and responsibilities, as well as detection and response procedures specific to Customer's organization.

SecureWorks will request documentation that supports the effort to understand Customer's current posture and practices in order to draft IR materials tailored to Customer's organization. The documentation requested will consist of items such as process diagrams, policies, procedures, guidelines and any other pertinent information necessary to help SecureWorks to understand current practices and regulatory requirements. As deemed necessary, facilitated workshops and interviews may also be conducted with Customer key stakeholders to rapidly gather a deeper understanding of overall requirements, critical business requirements and existing response capabilities. It is anticipated that Customer's Engagement point of contact will provide the requested information and access to key stakeholders as rapidly as possible once the Engagement begins.

Please note that this Engagement requires ample commitment and participation by Customer representatives by actively participating in the development process, providing information in a timely manner and reviewing drafted content to confirm the material is suitable for Customer's organization.

SecureWorks will create IR Plans incorporating any previously available content that may include the following sections:

- IR Charter
- Delineation of Roles, Responsibilities, Dependencies and Levels of Authority for Incidents
- Incident Categorization and Severity Definitions
- Procedural Flows and Escalation Procedures for Incident Handling
 - Event Detection Process
 - Triage and Analysis Process
 - Incident Declaration Process
 - IR and Recovery Process
 - Incident Communication Process
- Reporting Procedures, Templates and Forms
- Response Team, Key Vendor and Law Enforcement Contact Information
- Internal and External Notification Requirements
- Employee Awareness and Readiness Training
- Post-Incident Analysis and Improvement Process
- IR Metrics

Compromise Screening Assessment

Upon SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks will perform compromise screening assessments that may include the analysis of log data, packet captures and forensically acquired images from key devices within Customer's infrastructure.

These artifacts will be analyzed for signs indicative of compromise activity. Artifacts will be analyzed as needed, based on availability and relevance to the assessment scope and required work effort. The data from these artifacts will be screened for threat indicators using a combination of publically available and SecureWorks proprietary tools and methods. These proprietary tools and methods will be used to identify patterns of behavior and communications that may indicate unknown compromise activity. Any log data should be provided to SecureWorks in a clear text format that enables the application of threat intelligence. The storage size of artifacts to be analyzed will be assumed to be the actual, uncompressed volume of data when estimating level of effort.

As deemed necessary and appropriate, SecureWorks may deploy live network traffic analysis appliances on Customer's network to obtain a network-centric view of live traffic with the aim of identifying active connections to known malicious addresses, command and control servers and traffic patterns representative of malware.

To deploy these live network traffic analysis appliances, SecureWorks will work with Customer's personnel to select appropriate network locations that will inspect as much "host-to-Internet" traffic as possible so that an appropriate amount of data is collected and analyzed. The live network traffic analysis appliances will only operate in detection mode and not alter or block any traffic during the Engagement.

The design and placement of the live network traffic analysis appliances will be verified in the early stages of the Engagement and may consist of one or more sensor live network traffic analysis appliances. Customer personnel must perform minor network configuration changes to accommodate network traffic analysis. Management and analysis access to the sensors live network traffic analysis appliances will be finalized during the pre-deployment phase. SecureWorks will manage and operate the live network traffic analysis appliances for the duration of the Engagement.

When any compromise activity is identified, SecureWorks can help plan containment and eradication or conduct post-incident forensic analysis. At the close of the assessment, Customer will receive a findings and recommendations report that includes any compromise activity observed and recommendations to improve IR practices.

Incident Management Risk Assessment

Upon SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks will conduct an operational and technical risk assessment of Customer's incident management capabilities to detect and mitigate malicious threat actors and commonly exploited threat vectors. An operational review will be conducted to assess current IR practices and measure capability maturity relative to SecureWorks' breadth of experience for threat scenarios of concern. A technical review can also be performed to validate IR operational practices and identify any gaps in compromise detection capabilities. The Incident Management Risk Assessment can inform any modifications required for IR strategy, plans, playbooks and testing practices. When any compromise activity is identified during the technical review, SecureWorks will help plan containment and eradication or conduct post-incident forensic analysis. At the close of the Engagement, Customer will receive a risk prioritized findings and recommendations report to improve IR practices.

Reactive Service Options

Reactive Incident Management Services are included as part of the Incident Management Retainer. Cook County will have access to both Proactive & Reactive Services with the current 80 Hour retainer to be use as requested throughout the year. If further hours are needed, Cook County can obtain these in blocks of 20 hours at the same defined rate of \$350.00/hr.

Digital Forensics and Incident Response Services

Upon SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks can provide Digital Forensics and Incident Response ("DFIR") Services. Once an incident is declared by Customer

and depending on the circumstances of the incident, SecureWorks can provide onsite or remote support.

In order to maintain independence during the investigation, SecureWorks **will not** perform remediation activities. This includes the removal or cleaning of any identified malicious code or root kits, or any other similar items. SecureWorks can assist in the development of remediation plans to address immediate weaknesses intended to limit the extent of the incident and minimize the potential for additional loss or damage.

Incident Response Services

SecureWorks Incident Handler(s) may attempt to establish all or part of the following:

- Provide written and/or verbal guidance for Customer artifact collection.
- Provide chain of custody procedures and documentation.
- Provide guidance and/or recommendations on remediating vulnerabilities discovered.
- Conduct forensic analysis of hard drive(s) from Customer environment that the incident affected.
- Conduct memory analysis of computer systems from Customer environment that the incident may have affected.
- Conduct analysis of mobile devices from Customer's environment that the incident may have affected.
- Conduct analysis of Credit Card end-point devices from Customer's environment that necessitate forensic review.
- Analysis of network traffic traversing internal or external boundaries.
- Perform custom searches based on key terms, user names, registry entries, file names, file types and/or time frame of interest.
- Analysis of network or system log events related to the Customer incident.
- Assessment of any recent vulnerability scans, penetration tests, web application tests, to assist in determining the unauthorized point(s) of entry.
- Conduct analysis of open source and proprietary Threat Intelligence sources that may provide information about threats, vulnerabilities, or risks related to the incident.
- Conduct analysis of malware or other binary files that may be involved in the incident.
- Provide indicators of the incident and threat for use by Customer remediating the incident.
- Provide any evidence discovered that indicates the likeness of the threat of concern.
- Incident summary and recommendations on risk management options.
- Provide media disposition per mutually agreed upon process. Additional costs may apply.

Digital Forensic Analysis Services

Using a variety of forensics tools and methods, SecureWorks can acquire, analyze and recover data stored in the following formats:

- Disk drives
- RAID systems
- Portable storage drives
- Credit card skimmers
- Mobile devices
- Other digital media formats for analysis or data recovery

Anti-Phishing Response Services

SecureWorks security analysts can analyze Phishing incidents. This can involve a variety of methodologies, depending on the nature of the incident. The objective is to gain as much information as possible about the incident to facilitate containment. A partial list of techniques includes:

- Networking analysis techniques (traceroute, DNS lookups, ARIN searches, OS fingerprinting, scanning, system enumeration, foot-printing, etc.).
- Application analysis techniques: website code reviews, email analysis, server configuration, etc.
- Research, including IRC, USENET, Websites.
- Analysis of propagation methodologies and magnitudes (i.e., how is the Phishing incident being spread?).
- Severity Assessment, including analysis of the impact of the incident.
- Log review—web logs, server logs, firewall logs, etc.
- Reverse lookup phone numbers used in attacks.
- Notification to mobile phone ISPs.
- Toll free reverse lookup.

No commitments of Customer resources will be made without clear consent from authorized Customer personnel. With guidance and consent from Customer management where needed, SecureWorks will coordinate, manage and facilitate an appropriate selection of countermeasures to have the Phishing site taken offline. These countermeasures will be selected and deployed dependent on the evolving analysis of the particular incident underway. Successful takedown is often dependent on cooperation of third parties such as internet service providers (“ISPs”), hosting providers, and domain registrars, among others. SecureWorks does not take offensive measure to takedown phishing sites.

Incident Coordination Services

In addition to performing incident handling and digital forensic analysis services, SecureWorks can provide advisory Services in the analysis and handling of incidents. During IR, SecureWorks often collaborates with executive teams, legal, public relations and other Customer key stakeholders. SecureWorks’ role is to provide these key stakeholders findings and impact assessments derived from IR and forensics work effort. These coordination activities may include:

- Coordinating the Engagement in-brief and regular status meetings.
- Scope definition and management during the course of the Engagement.
- Engagement staff and resource management.
- Engagement status reporting.
- Engagement deliverable reporting.
- Engagement support with the Customer and through the Customer, with other third parties.

Cloud Incident Response Services

SecureWorks will provide IR Services for the coordination, analysis, and handling of incidents involving the Customer Cloud Computing architecture. The Service will review evidence of compromise activity that can exist in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) Cloud Computing architectures. SecureWorks IR personnel can perform investigations to determine nature and extent of suspected intrusions involving Public, Private, and Hybrid Cloud Computing architectures with the Customer and through the Customer when they are end users of Cloud Service Providers (CSPs). Cloud IR Services are highly dependent on prevailing organizational, legal, and technical factors that may complicate investigations involving the Customer Cloud Computing architecture and are conducted on a commercially reasonable effort basis.

Optional Premium Services

In the event that services hereunder ("Premium Services") are required to assist in the delivery of any incident response services, Premium Services will be billed at the **Premium Services Rate** outlined in Section 5.10. SecureWorks will not perform Premium Services work without prior customer notification, acceptance, and approval. Retained hours at the Standard Retainer Rate may be applied to Premium Services based on a factor to convert those hours to the nearest half hour increment (standard premium hour rate is \$500/hr).

Advanced Malware Analysis and Reverse Engineering Services

In the event of a malicious code infection of an unknown type, SecureWorks can attempt to reverse engineer the code to better understand the code's capabilities. SecureWorks has extensive experience and expertise in malware reverse engineering, but this activity is conducted on a commercially reasonable effort basis because not all code can be successfully reverse-engineered. SecureWorks will offer an opinion on the code's potential impact and effect on Customer assets.

Incident Surveillance Services

In an effort to ascertain additional information about the attack source and methods, SecureWorks will attempt to:

- Find specific references to Customer assets affected by the current attack within underground communications.
- Identify specific references to Customer assets in attack tools or malware "kits."
- Research historic proprietary and public data regarding targeted attacks against Customer assets.
- Monitor and analyze underground communications pertaining to the active attack.

Customer will work with SecureWorks to provide specific information on the assets to be covered under this project (e.g., names, identifiers, IP address ranges, brands, etc.) for correlation in counterintelligence during the active attack phase.

Targeted Threat Hunting and Response

Upon SecureWorks' receipt of a Customer Authorized Engagement request, SecureWorks can perform a Targeted Threat Hunting and Response assessment, as set forth and described below, in the Customer environment. This service leverages SecureWorks' proprietary methodology, expertise and intelligence related to advanced threat actors and their techniques, tactics and procedures (TTP). Targeted Threat Hunting and Response is specifically designed for customers that need to understand their exposure to targeted threats, and attempts to identify existing adversary presence or tradecraft in the Customer environment. The service will review evidence that may persist in network infrastructure logs, and analyze endpoint systems and other relevant data stored within the organization, to identify indicators of intrusion. When intrusions are identified, SecureWorks can help plan and execute threat actor containment and eradication. At the close of the Engagement, Customer will receive a findings and recommendations report that includes any targeted threat activity observed and recommendations to improve IR practices.

The following methods may be used by the Consultants for this Engagement. These method descriptions are provided to describe the techniques that may be used, as agreed upon with the Customer. These methods are not in scope unless identified in the Scope of Work defined in the Engagement request order in a format substantially similar to **Appendix A**, but may be added by the methods listed in the **Service Fees and Expenses** section below.

NOTE: This service requires a minimum of 80 hours of Premium Services at the Premium Services Rate as defined in Section 5.10.

Pre-Engagement Planning

Prior to the Engagement, the Customer will provide the assigned SecureWorks team members with a completed Targeted Threat Hunting and Response Service Questionnaire and the required supporting documentation, including host and network architecture information. SecureWorks will work with the customer to identify data necessary to complete the assessment and identify available sources of required data, or formulate a plan to obtain the required data. This information will be thoroughly reviewed to prepare SecureWorks consultants for the Engagement.

Additional environment instrumentation (IDS/IPS, etc.) may be required to obtain the necessary data, and in these cases, SecureWorks will work with the Customer to identify options they can implement prior to the Engagement. If additional instrumentation is required to effectively perform the Engagement, the project start may be delayed.

As deemed necessary and appropriate, the Engagement may commence with a workshop involving the Customer's IT security staff and the SecureWorks consultants to further collect environmental specifics and calibrate Engagement objectives.

Log Assessment

The service includes the analysis of log data from key technical elements within the Customer's network. The logs will be analyzed for entries indicative of the operation of malicious software or threat actor activity. Logs will be analyzed as needed, based on availability and relevance to the assessment work.

The data from these logs will be screened for targeted threat and malware indicators using a mixture of publically available and SecureWorks proprietary tools. These tools will be used to identify patterns of behavior and communications with suspicious IP addresses that may indicate the presence of malware. Due to the complexity of the search algorithms and the size of the databases behind them, some of this processing work will need to be carried out on SecureWorks' owned and operated platforms.

Logs should be provided to SecureWorks on disk or other storage media, or alternatively made available in a form that enables them to write code to apply intelligence to the logs in an encrypted format. The storage size of logs to be analyzed will be assumed to be the actual, uncompressed volume when estimating the scope of work effort.

Network Traffic Analysis

As deemed necessary and appropriate, SecureWorks may deploy live network traffic analysis ("Network Traffic Analysis") appliances on Customer's network to obtain a network-centric view of live traffic with the aim of identifying active connections to known malicious addresses, command and control servers, and traffic patterns that are representative of known malware.

To deploy the appliances, SecureWorks will work with Customer to select appropriate network locations that will inspect as much "host-to-Internet" traffic as possible so that an appropriate amount of data is collected and analyzed. The live Network Traffic Analysis appliances will only operate in detection mode and not alter or block any traffic during the Engagement. SecureWorks will deploy a maximum of two appliances in Customer's network. Additional appliances can be deployed for an additional fee; we will work with Customer to determine if additional appliances are required.

The design and placement of the live network traffic analysis appliances will be verified in the early stages of the Engagement and may consist of one or more sensor live network traffic analysis appliances. Customer personnel must perform minor network configuration changes to accommodate network traffic analysis. Management and analysis access to the sensors live network traffic analysis appliances will be finalized during the pre-deployment phase. SecureWorks will manage and operate the live network traffic analysis appliances for the duration of the Engagement.

Endpoint Assessment – Malware Hunting

The purpose of the malware hunting portion of the Engagement is to search systems within scope for threat indicators. Based on the results, hosts will be categorized as confirmed compromised, exhibiting suspicious threat indicators or exhibiting no known threat indicators. SecureWorks will conduct the following activities for the malware hunting exercise:

- Coordinate with the Customer team to execute the scans using one of several methodologies for connecting to the systems within scope.
- Run sample test scans to ensure the methodology is suitable for the target environment.
- Scan systems for Threat Indicators using a combination of proprietary SecureWorks tools, processes and intelligence.
- Receive scan results into an agreed upon and established repository.
- Review the scan results using threat intelligence, filter logic and established methodology.
- Refine Threat Indicator set as necessary based on findings from initial scans.
- Investigate any suspicious indicators/systems.
- Working iteratively, we will repeat certain steps above, to categorize the systems according to their level of risk/suspicion.
- Prepare findings for Customer including systems scanned, detected indicators and follow-up actions.

Containment and Response

Once sufficient evidence has been collected, the SecureWorks team will help define a customized containment and eradication plan. This plan is developed in preparation for rapid execution across the organization during a specified timeframe, locking down systems and adversary access in a swift motion. This plan is also likely to include a strategy to monitor for the adversary's attempts to re-enter Customer systems. All plans and work effort will be developed with the Customer and approved by Customer prior to execution.

1 Appendix A: SAMPLE Engagement Request for Incident Management Services

[REDACTED]

[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	

[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	

[REDACTED]

EXHIBIT 2

Schedule of Compensation

Advanced Security Services		Description	Quantity	Year 1	Year 2	Year 3
Dell SecureWorks - MSSP						
24x7 Monitoring Only:						
24x7 Managed & Monitored						
SecureWorks Required Analysis Tools & Log Collection						
Threat Intelligence Optional Add-On		Advanced CTU MONTHLY SUPPORT HOURS	optional add-on			
Incident Management Services			80 Hrs (Blocks of 10 Hrs Can be Added)			
Minimum of 40 Hours per year, 80 Proposed						
Alerting & Reporting			included			
Training			included			
Total SecureWorks MSS						
Advanced Security Services		Description	Quantity	Year 1	Year 2	Year 3

Ascent Innovations - M/WBE

24x7 Monitoring, No Management

24x7 Monitoring, Only After Hours Management

24x7 Monitoring, 24x7 Management

Optional, 24x7 Monitoring, Only After Hours Management

Optional, 24x7 Monitoring, 24x7 Management

Total Ascent MSS		\$ 287,775.00	\$ 287,775.00	\$ 287,775.00
Ascent Innovations - M/WBE				
One-Time Implementation & Project Management Cost				
Dell SecureWorks - MSSP				
One-Time Project Management				
Implementation, Integration, & Performance Tuning and Optimization				
One-Time MSS Activation				

Total for One-Time Costs + Yearly

Performance Tuning

Total For all MSS Services

Travel Estimates

All Costs year 1

\$ 184,500.00

\$ 726,377.50

\$ 726,377.50

\$ 32,000.00

\$ 32,000.00

\$ 942,877.50

\$

\$

\$

\$

\$

\$

\$

\$

\$

\$

\$

\$

\$

EXHIBIT 3

Minority and Women Owned Business Enterprise Commitment



OFFICE OF CONTRACT COMPLIANCE

JACQUELINE GOMEZ

DIRECTOR

118 N. Clark, County Building, Room 1020 • Chicago, Illinois 60602 • (312) 603-5502

TONI PRECKWINKLE

PRESIDENT

**Cook County Board
of Commissioners**

RICHARD R. BOYKIN

1st District

ROBERT STEELE

2nd District

JERRY BUTLER

3rd District

STANLEY MOORE

4th District

DEBORAH SIMS

5th District

JOAN PATRICIA MURPHY

6th District

JESUS G. GARCIA

7th District

LUIS ARROYO, JR

8th District

PETER N. SILVESTRI

9th District

BRIDGET GAINER

10th District

JOHN P. DALEY

11th District

JOHN A. FRITCHEY

12th District

LARRY SUFFREDIN

13th District

GREGG GOSLIN

14th District

TIMOTHY O. SCHNEIDER

15th District

JEFFREY R. TOBOLSKI

16th District

SEAN M. MORRISON

17th District

May 27, 2016

Ms. Shannon E. Andrews
Chief Procurement Officer
118 N. Clark Street
County Building-Room 1018
Chicago, IL 60602

Re: Contract No. 1550-14939
Managed Security Service
Homeland Security and Emergency Management Department

Dear Ms. Andrews:

The following bid for the above-reference contract has been reviewed for compliance with the Minority and Women- owned Business Enterprises (MBE/WBE) Ordinance and have been found to be responsive to the Ordinance.

Bidder: SecureWorks, Inc.
Contract Value: \$2,459,632.50
Contract Goal: 35% MBE/WBE

<u>MBE/WBE</u>	<u>Status</u>	<u>Certifying Agency</u>	<u>Commitment</u>
Ascent Innovations, LLC	MBE/WBE-8	Cook County	38% (Direct)

The Office of Contract Compliance has been advised by the Requesting Department that no other bidders are being recommended for award. Revised MBE/WBE forms were used in the determination of the responsiveness of this contract.

Sincerely,

Jacqueline Gomez
Contract Compliance Director

JG/smp

cc: Toyla Rice, OCPO
Michael Herbstman, DHSEM

MBE/WBE UTILIZATION PLAN - FORM 1

BIDDER/PROPOSER HEREBY STATES that all MBE/WBE firms included in this Plan are certified MBEs/WBEs by at least one of the entities listed in the General Conditions - Section 19.

I. BIDDER/PROPOSER MBE/WBE STATUS: (check the appropriate line)

- ☒ Bidder/Proposer is a certified MBE or WBE firm. (If so, attach copy of current Letter of Certification)
- ☐ Bidder/Proposer is a Joint Venture and one or more Joint Venture partners are certified MBEs or WBEs. (If so, attach copies of Letter(s) of Certification, a copy of Joint Venture Agreement clearly describing the role of the MBE/WBE firm(s) and its ownership interest in the Joint Venture and a completed Joint Venture Affidavit - available online at www.cookcountylil.gov/contractcompliance)
- ☐ Bidder/Proposer is not a certified MBE or WBE firm, nor a Joint Venture with MBE/WBE partners, but will utilize MBE and WBE firms either directly or indirectly in the performance of the Contract. (If so, complete Sections II below and the Letter(s) of Intent - Form 2).

II. ☒ Direct Participation of MBE/WBE Firms ☐ Indirect Participation of MBE/WBE Firms

NOTE: Where goals have not been achieved through direct participation, Bidder/Proposer shall include documentation outlining efforts to achieve Direct Participation at the time of Bid/Proposal submission. Indirect Participation will only be considered after all efforts to achieve Direct Participation have been exhausted. Only after written documentation of Good Faith Efforts is received will Indirect Participation be considered.

MBEs/WBEs that will perform as subcontractors/suppliers/consultants include the following:

MBE/WBE Firm: Ascent Innovations LLC

Address: 475 N. Martingale Road Suite 820, Schaumburg IL 60173.

E-mail: sohena.hafiz@ascentinnov.com

Contact Person: Sohena Hafiz Phone: 847.572.8000

Dollar Amount Participation: \$ Please see sealed PRICE PROPOSAL

Percent Amount of Participation: _____

*Letter of Intent attached? Yes ☒ No ☐
*Current Letter of Certification attached? Yes ☒ No ☐

MBE/WBE Firm: _____

Address: _____

E-mail: _____

Contact Person: _____ Phone: _____

Dollar Amount Participation: \$ _____

Percent Amount of Participation: _____ %

*Letter of Intent attached? Yes ☐ No ☐
*Current Letter of Certification attached? Yes ☐ No ☐

Attach additional sheets as needed.

* Letter(s) of Intent and current Letters of Certification must be submitted at the time of bid.

MBE/WBE LETTER OF INTENT - FORM 2

MWBE Firm: Ascent Innovations LLC Certifying Agency: Cook County
 Contact Person: Sohena Hafiz Certification Expiration Date: 08/25/2016
 Address: 475 N. Martingale Road Suite 820 Ethnicity: South Asian
 City/State: Schaumburg, IL Zip: 60173 Bid/Proposal/Contract #: 1550-14939
 Phone: 847.572.8000 Fax: 866.681.9298 FEIN #: 27-1301225
 Email: sohena.hafiz@ascentinnov.com
 Participation: ☒ Direct ☐ Indirect

Will the MWBE firm be subcontracting any of the goods or services of this contract to another firm?

☒ No ☐ Yes - Please attach explanation. Proposed Subcontractor(s): _____

The undersigned MWBE is prepared to provide the following Commodities/Services for the above named Project/ Contract: (If more space is needed to fully describe MWBE Firm's proposed scope of work and/or payment schedule, attach additional sheets)

Ascent Innovations will provide management and
monitoring of security systems as a certified local
MBE/WBE subcontractor in conjunction with
Dell SecureWorks.

Indicate the Dollar Amount, Percentage, and the Terms of Payment for the above-described Commodities/ Services:

Please see PRICE PROPOSAL (SEALED)

THE UNDERSIGNED PARTIES AGREE that this Letter of Intent will become a binding Subcontract Agreement for the above work, conditioned upon (1) the Bidder/Proposer's receipt of a signed contract from the County of Cook; (2) Undersigned Subcontractor remaining compliant with all relevant credentials, codes, ordinances and statutes required by Contractor, Cook County, and the State to participate as a MBE/WBE firm for the above work. The Undersigned Parties do also certify that they did not affix their signatures to this document until all areas under Description of Service/ Supply and Fee/Cost were completed.

Sohena Hafiz
 Signature (MWBE)

Sohena Hafiz
 Print Name

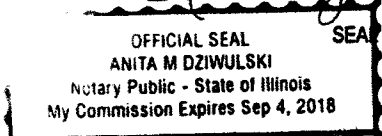
Ascent Innovations LLC
 Firm Name

11/18/2015
 Date

Subscribed and sworn before me

this 18 day of November, 2015.

Notary Public *Anita M Dziwulski*



M/WBE Utilization Plan - Form 2

David Baum
 Signature (Prime Bidder/Proposer)

DAVID BAUM
 Print Name

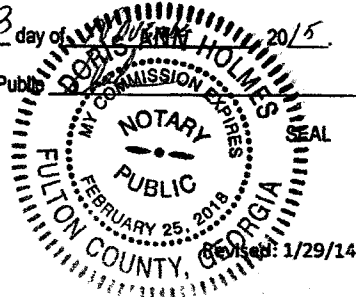
SECUREWORKS INC.
 Firm Name

11/23/15
 Date

Subscribed and sworn before me

this 23 day of November, 2015.

Notary Public *Donna Holmes*



Revised: 1/29/14



TONI PRECKWINKLE

PRESIDENT
Cook County Board
of Commissioners

RICHARD R. BOYKIN
1st District

ROBERT STEELE
2nd District

JERRY BUTLER
3rd District

STANLEY MOORE
4th District

DEBORAH SIMS
5th District

JOAN PATRICIA MURPHY
6th District

JESUS G. GARCIA
7th District

LUIS ARROYO, JR.
8th District

PETER N. SILVESTRI
9th District

BRIDGET GAINER
10th District

JOHN P. DALEY
11th District

JOHN A. FRITCHEY
12th District

LARRY SUFFREDIN
13th District

GREGG GOSLIN
14th District

TIMOTHY O. SCHNEIDER
15th District

JEFFREY R. TOBOLSKI
16th District

SEAN M. MORRISON
17th District

OFFICE OF CONTRACT COMPLIANCE

JACQUELINE GOMEZ

DIRECTOR

118 N. Clark, County Building, Room 1020 • Chicago, Illinois 60620 • (312) 603-5502

August 25, 2015

Ms. Sohena Hafiz, President
Ascent Innovations, LLC
475 North Maringale, Suite 820
Schaumburg, IL 60173

Annual Certification Expires: August 25, 2016

Dear Ms. Hafiz:

Congratulations on your continued eligibility for Certification as a Minority Business Enterprise/ Women Business Enterprise (MBE/WBE) by Cook County Government. This MBE/WBE Certification is valid until **August 25, 2019**.

As a condition of continued Certification, you must file a **"No Change Affidavit"** within **sixty (60) days** prior to the date of annual expiration. Failure to file this Affidavit shall result in the termination of your certification. You must notify Cook County Government's Office of Contract Compliance of any change in ownership or control or any other matters or facts affecting your firm's eligibility for Certification within **fifteen (15) business days** of such changes.

Cook County Government may commence action to remove your firm as a **MBE/WBE** vendor if you fail to notify us of any changes of facts affecting your firm's certification, or if your firm otherwise fails to cooperate with the County in any inquiry or investigation. Removal of status may also be commenced if your firm is found to be involved in bidding or contractual irregularities.

Your firm's name will be listed in Cook County's Directory of Minority Business Enterprise, Women Business Enterprise and/ or Veteran Business Enterprise in the area(s) of specialty:

TECHNOLOGY: SOFTWARE AND ENTERPRISE RESOURCE PLANNING (ERP) CONSULTING

Your firm's participation on County contracts will be credited toward **MBE** or **WBE** goals in your area(s) of specialty. While your participation on Cook County contracts is not limited to your specialty, credit toward **MBE** or **WBE** goals will be given only for work performed in the specialty category.

Thank you for your continued interest in Cook County Government's Minority, Women and Veteran Business Enterprise Programs.

Sincerely,

Jacqueline Gomez
Contract Compliance Director

JG/ehw

2019

I. POLICY AND GOALS

- A. It is the policy of the County of Cook to prevent discrimination in the award of or participation in County Contracts and to eliminate arbitrary barriers for participation in such Contracts by local businesses certified as a Minority Business Enterprise (MBE) and Women-owned Business Enterprise (WBE) as both prime and sub-contractors. In furtherance of this policy, the Cook County Board of Commissioners has adopted a Minority- and Women-owned Business Enterprise Ordinance (the "Ordinance") which establishes annual goals for MBE and WBE participation as outlined below:

Contract Type	Goals	
	MBE	WBE
Goods and Services	25%	10%
Construction	24%	10%
Professional Services	35% Overall	

- B. **The County shall set contract-specific goals, based on the availability of MBEs and WBEs that are certified to provide commodities or services specified in this solicitation document. The MBE/WBE participation goals for this Agreement is 35% Overall.** A Bid, Quotation, or Proposal shall be rejected if the County determines that it fails to comply with this General Condition in any way, including but not limited to: (i) failing to state an enforceable commitment to achieve for this contract the identified MBE/WBE Contract goals; or (ii) failing to include a Petition for Reduction/Waiver, which states that the goals for MBE/WBE participation are not attainable despite the Bidder or Proposer Good Faith Efforts, and explains why. If a Bid, Quotation, or Proposal is rejected, then a new Bid, Quotation, or Proposal may be solicited if the public interest is served thereby.
- C. To the extent that a Bid, Quotation, or Proposal includes a Petition for Reduction/Waiver that is approved by the Office of Contract Compliance, the Contract specific MBE and WBE participation goals may be achieved by the proposed Bidder or Proposer's status as an MBE or WBE; by the Bidder or Proposer's enforceable joint-venture agreement with one or more MBEs and/or WBEs; by the Bidder or Proposer entering into one or more enforceable subcontracting agreements with one or more MBE and WBE; by the Bidder or Proposer establishing and carrying out an enforceable mentor/protégé agreement with one or more MBE and WBE; by the Bidder or Proposer actively engaging the Indirect Participation of one or more MBE and WBE in other aspects of its business; or by any combination of the foregoing, so long as the Utilization Plan evidences a commitment to meet the MBE and WBE Contract goals set forth in (B) above, as approved by the Office of Contract Compliance.
- D. A single Person, as defined in the Procurement Code, may not be utilized as both an MBE and a WBE on the same Contract, whether as a Consultant, Subcontractor or supplier.

- E. Unless specifically waived in the Bid or Proposal Documents, this Exhibit; the Ordinance; and the policies and procedures promulgated thereunder shall govern. If there is a conflict between this Exhibit and the Ordinance or the policies and procedures, the Ordinance shall control.
- F. A Consultant's failure to carry out its commitment regarding MBE and WBE participation in the course of the Contract's performance may constitute a material breach of the Contract. If such breach is not appropriately cured, it may result in withholding of payments under the Contract, contractual penalties, disqualification and any other remedy provided for in Division 4 of the Procurement Code at law or in equity.

II. REQUIRED BID OR PROPOSAL SUBMITTALS

A Bidder or Proposer shall document its commitment to meeting the Contract specific MBE and WBE participation goals by submitting a Utilization Plan with the Bid or Proposal. The Utilization Plan shall include (1) one or more Letter(s) of Intent from the relevant MBE and WBE firms; and (2) current Letters of Certification as an MBE or WBE. Alternatively, the Bidder or Proposer shall submit (1) a written Petition for Reduction/Waiver with the Bid, Quotation or Proposal, which documents its preceding Good Faith Efforts and an explanation of its inability to meet the goals for MBE and WBE participation. The Utilization Plan shall be submitted at the time that the bid or proposal is due. **Failure to include a Utilization Plan will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.**

A. MBE/WBE Utilization Plan

Each Bid or Proposal shall include a complete Utilization Plan, as set forth on Form 1 of the M/WBE Compliance Forms. The Utilization Plan shall include the name(s), mailing address, email address, and telephone number of the principal contact person of the relevant MBE and WBE firms. If the Bidder or Proposer submits a Bid or Proposal, and any of their subconsultants, suppliers or consultants, are certified MBE or WBE firms, they shall be identified as an MBE or WBE within the Utilization Plan.

1. Letter(s) of Intent

Except as set forth below, a Bid or Proposal shall include, as part of the Utilization Plan, one or more Letter(s) of Intent, as set forth on Form 2 of the M/WBE Compliance Forms, executed by each MBE and WBE and the Bidder or Proposer. The Letter(s) of Intent will be used to confirm that each MBE and WBE shall perform work as a Subcontractor, supplier, joint venture, or consultant on the Contract. Each Letter of Intent shall indicate whether and the degree to which the MBE or WBE will provide goods or services directly or indirectly during the term of the Contract. The box for direct participation shall be marked if the proposed MBE or WBE will provide goods or services directly related to the scope of the Contract. The box for Indirect participation shall be marked if the proposed MBE or WBE will not be directly involved in the Contract but will be utilized by the Bidder or Proposer for other services not related to the Contract. Indirect

Participation shall not be counted toward the participation goal. Each Letter of Intent shall accurately detail the work to be performed by the relevant MBE or WBE firm, the agreed dollar amount, the percentage of work, and the terms of payment.

Failure to include Letter(s) of Intent will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.

All Bids and Proposals must conform to the commitments made in the corresponding Letter(s) of Intent, as may be amended through change orders.

The Contract Compliance Director may at any time request supplemental information regarding Letter(s) of Intent, and such information shall be furnished if the corresponding Bid or Proposal is to be deemed responsive.

2. Letter(s) of Certification

Only current Letter(s) of Certification from one of the following entities may be accepted as proof of certification for MBE/WBE status, provided that Cook County's requirements for certification are met:

- County of Cook
- City of Chicago

Persons that are currently certified by the City of Chicago in any area other than Construction/Public Works shall also complete and submit a MBE/WBE Reciprocal Certification Affidavit along with a current letter of certification from the City of Chicago. This Affidavit form can be downloaded from www.cookcountyl.gov/contractcompliance.

The Contract Compliance Director may reject the certification of any MBE or WBE on the ground that it does not meet the requirements of the Ordinance, or the policies and rules promulgated thereunder.

3. Joint Venture Affidavit

In the event a Bid or Proposal achieves MBE and/or WBE participation through a Joint Venture, the Bid or Proposal shall include the required Joint Venture Affidavit, which can be downloaded from www.cookcountyl.gov/contractcompliance. The Joint Venture Affidavit shall be submitted with the Bid or Proposal, along with current Letter(s) of Certification.

B. Petition for Reduction/Waiver

In the event a Bid or Proposal does not meet the Contract specific goals for MBE and WBE participation, the Bid or Proposal shall include a Petition for Reduction/Waiver, as set forth on Form 3. The Petition for Reduction/Waiver shall be supported by sufficient

evidence and documentation to demonstrate the Bidder or Proposer's Good Faith Efforts in attempting to achieve the applicable MBE and WBE goals, and its inability to do so despite its Good Faith Efforts.

Failure to include Petition for Reduction/Waiver will render the submission not Responsive and shall be cause for the CPO to reject the Bid or Proposal.

III. REDUCTION/WAIVER OF MBE/WBE GOALS

A. Granting or Denying a Reduction/Waiver Request.

1. The adequacy of the Good Faith Efforts to utilize MBE and WBE firms in a Bid or Proposal will be evaluated by the CCD under such conditions as are set forth in the Ordinance, the policies and rules promulgated thereunder, and in the "Petition for Reduction/Waiver of MBE/WBE Participation Goals" – Form 3 of the M/WBE Compliance Forms.
2. With respect to a Petition for Reduction/Waiver, the sufficiency or insufficiency of a Bidder or Proposer's Good Faith Efforts shall be evaluated by the CCD as of the date upon which the corresponding Bid or Proposal was due.
3. The Contract Compliance Director or his or her duly authorized Waiver Committee may grant or deny the Petition for Reduction/Waiver based upon factors including but not limited to: (a) whether sufficient qualified MBE and WBE firms are unavailable despite good faith efforts on the part of the Bidder or Proposer; (b) the degree to which specifications and the reasonable and necessary requirements for performing the Contract make it impossible or economically infeasible to divide the Contract into sufficiently small tasks or quantities so as to enable the Bidder or Proposer to utilize MBE and WBE firms in accordance with the applicable goals; (c) the degree to which the prices or prices required by any potential MBE or WBE are more than 10% above competitive levels; and (d) such other factors as are determined relevant by the Contract Compliance Director or the duly authorized Waiver Committee.
4. If the Contract Compliance Director or the duly authorized Waiver Committee determines that the Bidder or Proposer has not demonstrated sufficient Good Faith Efforts to meet the applicable MBE and WBE goals, the Contract Compliance Director or the duly authorized Waiver Committee may deny a Petition for Reduction/Waiver, declare the Bid or Proposal non-responsive, and recommend rejection of the Bid, Quotation, or Proposal.

IV. CHANGES IN CONSULTANT'S UTILIZATION PLAN

- A. A Consultant, during its performance of the Contract, may not change the original MBE or WBE commitments specified in the relevant Utilization Plan, including but not limited to, terminating a MBE or WBE Contract, reducing the scope of the work to be performed by a MBE/WBE, or decreasing the price to a MBE/WBE, except as

otherwise provided by the Ordinance and according to the policies and procedures promulgated thereunder.

- B. Where a Person listed under the Contract was previously considered to be a MBE or WBE but is later found not to be, or work is found not to be creditable toward the MBE or WBE goals as stated in the Utilization Plan, the Consultant shall seek to discharge the disqualified enterprise, upon proper written notification to the Contract Compliance Director, and make every effort to identify and engage a qualified MBE or WBE as its replacement. Failure to obtain an MBE or WBE replacement within 30 business days of the Contract Compliance Director's written approval of the removal of a purported MBE or WBE may result in the termination of the Contract or the imposition of such remedy authorized by the Ordinance, unless a written Petition for Reduction/Waiver is granted allowing the Consultant to award the work to a Person that is not certified as an MBE or WBE.

V. NON-COMPLIANCE

If the CCD determines that the Consultant has failed to comply with its contractual commitments or any portion of the Ordinance, the policies and procedures promulgated thereunder, or this Exhibit, the Contract Compliance Director shall notify the Consultant of such determination and may take any and all appropriate actions as set forth in the Ordinance or the policies and procedures promulgated thereunder which includes but is not limited to disqualification, penalties, withholding of payments or other remedies in law or equity.

VI. REPORTING/RECORD-KEEPING REQUIREMENTS

The Consultant shall comply with the reporting and record-keeping requirements in the manner and time established by the Ordinance, the policies and procedure promulgated thereunder, and the Contract Compliance Director. Failure to comply with such reporting and record-keeping requirements may result in a declaration of Contract default. Upon award of a Contract, a Consultant shall acquire and utilize all Cook County reporting and record-keeping forms and methods which are made available by the Office of Contract Compliance. MBE and WBE firms shall be required to verify payments made by and received from the prime Consultant.

VII. EQUAL EMPLOYMENT OPPORTUNITY

Compliance with MBE and WBE requirements will not diminish or supplant other legal Equal Employment Opportunity and Civil Rights requirements that relate to Consultant and Subcontractor obligations.

Any questions regarding this section should be directed to:
Contract Compliance Director
Cook County
118 North Clark Street, Room 1020
Chicago, Illinois 60602
(312) 603-5502

EXHIBIT 4

Evidence of Insurance



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

05/26/2016

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an **ADDITIONAL INSURED**, the policy(ies) must be endorsed. If **SUBROGATION IS WAIVED**, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER MARSH RISK & INSURANCE SERVICES 345 CALIFORNIA STREET, SUITE 1300 CALIFORNIA LICENSE NO. 0437153 SAN FRANCISCO, CA 94104 Attn: Shannon Walker - shannon.walker@marsh.com	CONTACT NAME:	
	PHONE (A/C, No, Ext): FAX (A/C, No):	
INSURED Dell Inc. and its Subsidiaries One Dell Way - RRI-50 Round Rock, TX 78682-7000	E-MAIL ADDRESS:	
	INSURER(S) AFFORDING COVERAGE	
	INSURER A: Commerce & Industry Insurance Company	NAIC #
	INSURER B: (See Attached)	
	INSURER C: Steadfast Insurance Company	26387
	INSURER D: National Union Fire Ins Co Pittsburgh PA	19445
	INSURER E:	
	INSURER F:	

COVERAGES**CERTIFICATE NUMBER:**

SEA-003046186-13

REVISION NUMBER: 4

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			GL3796534	03/01/2016	03/01/2017	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 5,000,000 PRODUCTS - COMP/OP AGG \$ 5,000,000
D	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS			CA1861277	03/01/2016	03/01/2017	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
D	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED RETENTION \$			19086834	03/01/2016	03/01/2017	EACH OCCURRENCE \$ 10,000,000 AGGREGATE \$ 10,000,000
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N <input checked="" type="checkbox"/> N	N/A	SEE FOLLOWING PAGE Workers Compensation excluded in ND, OH & WA	03/01/2016	03/01/2017	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
C	Professional/E&O/ Technology Errors & Omissions			IPR929660404	06/01/2015	12/01/2016	Each Claim/Aggregate (Claims Made) 10,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

The above referenced Errors and Omissions policy shall include technology/professional liability, and data protection liability (cyber liability) insurance providing protection against: (a) errors and omissions in the performance of professional services; (b) breaches of security; (c) violation or infringement of any right of privacy, breach of federal, state, or foreign security and/or privacy laws or regulations; and (d) data theft, damage, destruction, or corruption.

CERTIFICATE HOLDER**CANCELLATION**

Dell Inc. and its Subsidiaries One Dell Way - RRI-50 Round Rock, TX 78682-7000	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE of Marsh Risk & Insurance Services Stephanie Guaiumi <i>Stephanie Guaiumi</i>

© 1988-2014 ACORD CORPORATION. All rights reserved.



ADDITIONAL REMARKS SCHEDULE

Page 2 of 2

AGENCY MARSH RISK & INSURANCE SERVICES		NAMED INSURED Dell Inc. and its Subsidiaries One Dell Way - RRI-50 Round Rock, TX 78682-7000
POLICY NUMBER		
CARRIER	NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: 25 FORM TITLE: Certificate of Liability Insurance

DELL INC. - WORKERS COMPENSATION/EMPLOYERS LIABILITY; EFFECTIVE 3/1/2016 - EXPIRATION 3/1/2017

Insurer: New Hampshire Insurance Co. NAIC# 23841

WC015519233 - All Other States

WC015519237 - CA

WC015519235 - FL

WC015519234 - WI, WY, (EMPLOYERS LIABILITY ONLY FOR THE FOLLOWING STATES: ND, OH, WA)

WC015519232 - AK, AZ, IL, KY NC, NH, NJ, PA, UT, VA, VT

WC015519239 - ME

WC015519236 - OR

Insurer: Insurance Co. of the State of PA. NAIC# 19429

WC015519238 - MA

Memorandum of Insurance

MEMORANDUM OF INSURANCE					DATE	
					22-Jun-2016	
<p>This Memorandum is issued as a matter of information only to authorized viewers for their internal use only and confers no rights upon any viewer of this Memorandum. This Memorandum does not amend, extend or alter the coverage described below. This Memorandum may only be copied, printed and distributed within an authorized viewer and may only be used and viewed by an authorized viewer for its internal use. Any other use, duplication or distribution of this Memorandum without the consent of Marsh is prohibited. "Authorized viewer" shall mean an entity or person which is authorized by the insured named herein to access this Memorandum via https://online.marsh.com/marshconnectpublic/marsh2/public/moi?client=362542334. The information contained herein is as of the date referred to above. Marsh shall be under no obligation to update such information.</p>						
PRODUCER			COMPANIES AFFORDING COVERAGE			
Marsh USA Inc. dba Marsh Risk & Insurance Services ("Marsh")			Co. A Commerce & Industry Insurance Company			
INSURED			Co. B National Union Fire Ins Co Pittsburgh PA			
Dell Inc. and its Subsidiaries			Co. C Various - See additional information section below			
One Dell Way - RRI-50			Co. D Steadfast Insurance Company			
Round rock						
Texas 78682						
United States						
COVERAGES						
<p>THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS MEMORANDUM MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS</p>						
CO LTR	TYPE OF INSURANCE	POLICY NUMBER	POLICY EFFECTIVE DATE	POLICY EXPIRATION DATE	LIMITS LIMITS IN USD UNLESS OTHERWISE INDICATED	
A	GENERAL LIABILITY Commercial General Liability Occurrence	GL3796534	01-MAR-2016	01-MAR-2017	GENERAL AGGREGATE	USD 5,000,000
					PRODUCTS - COMP/OP AGG	USD 5,000,000
					PERSONAL AND ADV INJURY	USD 1,000,000
					EACH OCCURRENCE	USD 1,000,000
					FIRE DAMAGE (ANY ONE FIRE)	USD 1,000,000
					MED EXP (ANY ONE PERSON)	USD 5,000
B	AUTOMOBILE LIABILITY Any Auto Hired Autos Non-Owned Autos	CA1861277	01-MAR-2016	01-MAR-2017	COMBINED SINGLE LIMIT	USD 1,000,000
					BODILY INJURY (PER PERSON)	
					BODILY INJURY (PER ACCIDENT)	
					PROPERTY DAMAGE	

B	EXCESS LIABILITY Umbrella Form	19086834	01-MAR-2016	01-MAR-2017	EACH OCCURENCE	USD 5,000,000
					AGGREGATE	USD 5,000,000
	GARAGE LIABILITY				AUTO ONLY (PER ACCIDENT)	
					OTHER THAN AUTO ONLY:	
					EACH ACCIDENT	
					AGGREGATE	
C	WORKERS	WC015519233-	01-MAR-2016	01-MAR-2017		
C	COMPENSATION /	AOS/WC015519239-	01-MAR-2016	01-MAR-2017		
C	EMPLOYERS	ME	01-MAR-2016	01-MAR-2017	WORKERS COMP LIMITS	Statutory
C	LIABILITY	WC015519235-	01-MAR-2016	01-MAR-2017	EL EACH ACCIDENT	USD 1,000,000
	THE	FL/WC015519237-			EL DISEASE - POLICY LIMIT	USD 1,000,000
	PROPRIETOR /	CA			EL DISEASE - EACH EMPLOYEE	USD 1,000,000
	PARTNERS /	WC015519234-				
	EXECUTIVE	ND.OH.WA.WI.WY				
	OFFICERS ARE	WC015519238-MA				
	Included					
D	Professional/E&O	IPR929660404	01-JUN-2015	01-DEC-2016	Aggregate	USD 5,000,000

The Memorandum of Insurance serves solely to list insurance policies, limits and dates of coverage. Any modifications here to are not authorized.

The Memorandum of Insurance serves solely to list insurance policies, limits and dates of coverage. Any modifications here to are not authorized.

MEMORANDUM OF INSURANCE		DATE 22-Jun-2016
<p>This Memorandum is issued as a matter of information only to authorized viewers for their internal use only and confers no rights upon any viewer of this Memorandum. This Memorandum does not amend, extend or alter the coverage described below. This Memorandum may only be copied, printed and distributed within an authorized viewer and may only be used and viewed by an authorized viewer for its internal use. Any other use, duplication or distribution of this Memorandum without the consent of Marsh is prohibited. "Authorized viewer" shall mean an entity or person which is authorized by the insured named herein to access this Memorandum via https://online.marsh.com/marshconnectpublic/marsh2/public/moi?client=362542334. The information contained herein is as of the date referred to above. Marsh shall be under no obligation to update such information.</p>		
PRODUCER Marsh USA Inc. dba Marsh Risk & Insurance Services ("Marsh")	INSURED Dell Inc. and its Subsidiaries One Dell Way - RRI-50 Round rock Texas 78682 United States	
ADDITIONAL INFORMATION WORK COMP POLICIES -		

New Hampshire Insurance Co.

WC015519233 - All Other States

WC015519235 - FL

WC015519237 - CA

WC015519236 - OR

WC015519234 - ND, OH, WA, WI, WY

WC017731509 - AK, AZ, IL, KY, NC, NH, NJ, PA, UT, VA, VT

WC015513239 - ME

Insurance Co. of the State of PA

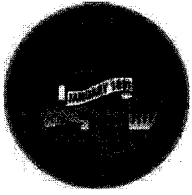
WC015519238 - MA

ADDITIONAL INSURED APPLIES WHERE REQUIRED BY WRITTEN CONTRACT. WAIVER OF
SUBROGATION APPLIES WHERE REQUIRED BY CONTRACT AND WHERE PERMITTED BY LAW.

The Memorandum of Insurance serves solely to list insurance policies, limits and dates of
coverage. Any modifications hereto are not authorized.

EXHIBIT 5

Board Authorization



Board of Commissioners of Cook County

118 North Clark Street
Chicago, IL

Legislation Details

File #:	16-3335	Version:	1	Name:	SecureWorks, Inc., Atlanta, Georgia
Type:	Contract	Status:		Status:	Approved
File created:	5/18/2016	In control:		In control:	Board of Commissioners
On agenda:	7/13/2016	Final action:		Final action:	7/13/2016
Title:	PROPOSED CONTRACT (TECHNOLOGY)				

Department(s): Homeland Security and Emergency Management

Vendor: SecureWorks, Inc., Atlanta, Georgia

Request: Authorization for the Chief Procurement Officer to enter into and execute contract

Good(s) or Service(s): Managed Security Services Integration

Contract Value: \$2,459,632.50

Contract period: 7/13/2016 - 7/12/2019 with two (2) one (1) year renewal options

Potential Fiscal Year Budget Impact: FY 2016 \$563,689.75 in grant funds, FY 2017 \$758,377.50 in grant funds, FY 2018 \$758,377.50 in grant funds and FY 2019 \$379,188.75 in grant funds

Accounts: 769 - N/A

Contract Number(s): 1550-14939

Concurrence(s):

The vendor has met the Minority and Women Owned Business Enterprise Ordinance via direct participation.

The Chief Procurement Officer concurs.

The Bureau of Technology concurs

Summary: SecureWorks Inc. is a managed security service provider (MSSP). It provides information security services, protecting its customers' computers, networks and information assets from malicious activity such as cybercrime. This contract will provide the County with round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies. Further, it will address information security concerns such as targeted malware, data theft, skills shortages and resource constraints.

This contract is awarded through Request for Proposals (RFP) procedures in accordance with Cook County Procurement Code. SecureWorks, Inc. was selected based on established evaluation criteria.

Sponsors:

Indexes: ERNEST BROWN, Executive Director, Department of Homeland Security and Emergency Management

Code sections:

Attachments:

Date	Ver.	Action By	Action	Result
7/13/2016	1	Board of Commissioners	approved	Pass

EXHIBIT 6

Identification of Subcontractor/Supplier/Subconsultant Form

Cook County
Office of the Chief Procurement Officer
Identification of Subcontractor/Supplier/Subconsultant Form

OCPO ONLY:

- ☐ Disqualification
☐ Check Complete

The Bidder/Proposer/Respondent ("the Contractor") will fully complete and execute and submit an Identification of Subcontractor/Supplier/Subconsultant Form ("ISF") with each Bid, Request for Proposal, and Request for Qualification. **The Contractor must complete the ISF for each Subcontractor, Supplier or Subconsultant which shall be used on the Contract.** In the event that there are any changes in the utilization of Subcontractors, Suppliers or Subconsultants, the Contractor must file an updated ISF.

Bid/RFP/RFQ No.: 1550-14939	Date: July 15th, 2016
Total Bid or Proposal Amount: \$2,459,632.50 over 3 years	Contract Title: Managed Security Services Provider MSSP
Contractor: SecureWorks	Subcontractor/Supplier/ Subconsultant to be added or substitute: Ascent Innovations
Authorized Contact for Contractor: Taylor Murphy	Authorized Contact for Subcontractor/Supplier/ Subconsultant: Robert Sterling
Email Address (Contractor): Taylor_Murphy@Dell.com	Email Address (Subcontractor): robert.sterling@ascentinnov.com
Company Address (Contractor): One Concourse Pkwy Suite 500	Company Address (Subcontractor): 475 North Martingdale #820
City, State and Zip (Contractor): Atlanta, GA 30328	City, State and Zip (Subcontractor): Schaumburg, IL 60173
Telephone and Fax (Contractor) 770-868-6434, Fax: 404-728-0144	Telephone and Fax (Subcontractor) 847-572-8000, Fax: 866-681-9298
Estimated Start and Completion Dates (Contractor) July 15, 2016	Estimated Start and Completion Dates (Subcontractor) July 15, 2019 unless extended

Note: Upon request, a copy of all written subcontractor agreements must be provided to the OCPO.

<u>Description of Services or Supplies</u>	<u>Total Price of Subcontract for Services or Supplies</u>
24x7 or after-hours only Monitoring and/or Management of Security Devices & Technologies	\$956,425 over 3 years

The subcontract documents will incorporate all requirements of the Contract awarded to the Contractor as applicable. The subcontract will in no way hinder the Subcontractor/Supplier/Subconsultant from maintaining its progress on any other contract on which it is either a Subcontractor/Supplier/Subconsultant or principal contractor. This disclosure is made with the understanding that the Contractor is not under any circumstances relieved of its abilities and obligations, and is responsible for the organization, performance, and quality of work. **This form does not approve any proposed changes, revisions or modifications to the contract approved MBE/WBE Utilization Plan. Any changes to the contract's approved MBE/WBE/Utilization Plan must be submitted to the Office of the Contract Compliance.**

Contractor Cheryl Strack

Name Contracts Senior Advisor

Title 

Prime Contractor Signature

7/22/2016

Date

1550-14939

EXHIBIT 7

Cook County Travel and Transportation Policy



COOK COUNTY TRANSPORTATION EXPENSE REIMBURSEMENT AND TRAVEL REGULATIONS POLICY

Adopted: FY2009

COOK COUNTY TRANSPORTATION EXPENSE REIMBURSEMENT

SECTION I. AUTOMOBILE REIMBURSEMENT PLAN

- A. Any employee who is required and authorized to use their personally owned automobile in the conduct of official County Business shall be allowed and reimbursed. The number of County business miles driven per ½ month will be compensated at the standard IRS deduction for business related transportation currently in effect and authorized by the Bureau of Administration. IRS mileage rates adjusted midyear will not be made retroactive.
- B. In addition, parking and tolls shall be allowed for reimbursement if items are supported by receipts. Proof of IPASS charges shall be submitted along with the Transportation Expense Voucher.

SECTION II. GUIDELINES

A. Commuting Expenses

Commuting expenses between an employee's home and regular place of assignment will not be reimbursed, even if an employee's regular place of assignment is at different locations on different days within the County.

***Example:** An employee working for the Assessor's Office is regularly assigned to the Assessor's Office in Markham on Mondays and to the Assessor's Office in Maywood on Tuesdays through Fridays. Travel expenses to and from the employee's home and Assessor's Office on any day will not be reimbursed when assignments are permanent.*

B. Temporary and Minor Assignments (residence to temporary duty point)

Employees who are required to perform County business in the form of temporary and minor assignments beyond the general area of their regular place of assignment in the County may be reimbursed for their transportation expenses between home and their first or last stop, for such travel attributed to County business.

Mileage to first stop or from last stop between home and temporary place of assignment may be allowed and reimbursed.

Authorization for reimbursement for transportation between home and first or last stop shall only be allowed when, in the judgment of the Department head, reporting to the regular place of assignment is not reasonable because of the elements of time, place, business purpose and employee effectiveness. The assignment must be temporary and not indefinite.

C. Temporary and Minor Assignments (mileage between temporary duty points)

Employees who receive one or more temporary assignments in a day may be reimbursed for transportation for getting from one place to the other. Mileage from the employee's regular place of assignment, or first duty point, to all temporary duty points and back to regular place of assignment, or last duty point, is entitled to reimbursement.

D. General Guidelines

1. Mileage must be computed on the basis of the most direct route. Any mileage incurred solely for personal reasons is not reimbursable.
2. Employees must bear the cost of their normal commuting expenses between residence and official place of assignment.
3. Close supervision shall be maintained over the use of privately owned vehicles by the Department Heads. Authorization for use of privately owned vehicles shall only be given when deemed a service and benefit to Cook County Government. Reimbursements for transportation shall only be as compensation for services performed for the County.

SECTION III. TRANSPORTATION EXPENSE VOUCHER

A. Preparation

1. All claims for compensation of transportation expenses including the use of privately owned automobile and incidental parking fees and tolls, and taxicab and bus fares shall be submitted and itemized in the Transportation Expense Voucher. (For each stop of business use, enter date, started from location, finished at location, miles and expense between each stop. Total the dollar amount and enter in the space for "Total.")
2. When travel between home and first or last temporary duty point is authorized, the employee's residence shall be entered on the Transportation Expense Voucher, "Started from Location" or "Finished at Location."
3. The Transportation Expense Voucher shall be supported by receipts for all items, individually.
4. The Transportation Expense Voucher shall be prepared and signed by the individual who has incurred the expense and signed by their Supervisor. The original Voucher shall be submitted to the Comptroller's Office and a copy should be retained by the employee and by the department. Falsification of a Transportation Expense Voucher is considered a major cause infraction subject to disciplinary action up to and including discharge.

5. The individual submitting the Transportation Expense Voucher is personally responsible for its accuracy and priority. Trip details shall be entered immediately following automobile use to eliminate possibility of errors. The form must be completed in its entirety, e.g., insurance coverage.

B. Approval and Submission

1. The Transportation Expense Voucher shall be approved by the Department Head or a designated representative, who shall sign the original copy of the Transportation Expense Voucher. The original Voucher shall be sent to the Comptroller's Office by the 10th day of the following month in which the travel expense was incurred. Transportation Expense Vouchers submitted 60 days after the end of the month in which travel expense was incurred will not be reimbursed. A copy of the Transportation Expense Voucher shall be retained by the department and the employee.
2. Any Transportation Expense Voucher not prepared in accordance with these regulations, including the proper signatures, will be returned to the originator for corrections.

C. Authorized Attendance at Seminars, Meetings, Conventions, etc., on County Business

These expenses shall be detailed in accordance with the procedure relating to "Cook County Travel Regulations."

SECTION IV. COUNTY-OWNED AUTOMOBILE

Section 162(a)(2) of the Internal Revenue Code requires that any employee who is assigned a County-owned vehicle for use in performance of the employee's duties and who uses the vehicle for use in performance of the employee's duties and who uses the vehicle to commute from home to work and/or from work to home must include in their compensation the value to the employee (as provided for by the IRS) for each day such vehicle is used for commuting purposes, and Cook County must include this compensation on employee W-2 form.

The use of County-owned vehicles for personal use is prohibited.

COOK COUNTY TRAVEL REGULATIONS

SECTION I

TRAVEL EXPENSES

- A.** Travel expenses are ordinary and necessary expenses for transportation, hotel accommodations, meals and incidental expenses for travel that is longer than an ordinary day's work, and the employee needs to get sleep or rest during non-working time while away.

Reimbursements shall be allowed if the following requirements are met:

1. Travel is for periods more than or equal to be employee's scheduled workdays hours, plus 2 hours (usually 10 hours).
2. The employee must get sleep or rest while away in order to complete County business. (This does not mean napping in the car.)
3. Lodging and air travel shall be arranged through a County travel vendor, as specified by the Purchasing Agent.

SECTION II

RESPONSIBILITY OF DEPARTMENT HEAD

- A.** The Department Head is responsible for the execution of all travel regulations as well as such other policies and guidelines regarding travel as published by the Bureau of Administration.
- B.** All travel subject to these regulations shall be authorized in advance by the Department Head in accordance with current County directives.
- C.** Each Department shall develop a system for the prior authorization and control of travel to prevent expenses exceeding appropriations and to hold travel to the minimum required for efficient and economical conduct of County business.
- D.** The rates for reimbursements set forth in these regulations represent the maximums permitted under IRS guidelines.

SECTION III

ALLOWABLE TRANSPORTATION EXPENSE

- A.** Modes of transportation authorized for official travel in the course of County business will include automobiles, railroads, airlines, buses, taxicabs, and other usual means of conveyance. Transportation may include fares and expenses incidental to transportation such as baggage transfer, official telephone messages in connection with items classed as transportation, and reasonable tips.
- B.** All taxicab fares shall be accompanied by a receipt indicating the amount paid.

- C. Transportation between place of lodging and place of business at a temporary work location shall be allowed as a transportation expense.

SECTION IV MODE OF TRAVEL

- A. All travel shall be by the most direct route.
- B. In cases where an individual for their own convenience travels by an indirect route or interrupts travel by direct route, that individual shall bear the extra expense. Reimbursement for expenses shall be based only on such charges as would have been incurred by the most direct and economical route.
- C. All travel shall be by the most economical mode of transportation available, considering travel time, costs, and work requirements.

SECTION V ACCOMMODATIONS ON AIRPLANES, TRAINS, AND BUSES

- A. First class travel is prohibited
- B. Travel on airplanes shall be coach class.
- C. Any charges incurred as a result of changes to an original airline reservation made prior to or during travel are subject to Department Head approval.

SECTION VI USE OF PRIVATELY OWNED OR RENTED CONVEYANCE

- A. When an individual rendering service to the County uses privately owned motor vehicles in the conduct of official business and such use is authorized or approved as advantageous to the County, payment shall be made on a mileage basis at rates not to exceed those published by the Bureau of Administration.
- B. Reimbursement for the cost of automobile parking fees and tolls shall be allowed. The fee for parking an automobile at a common carrier terminal, or other parking area, while the traveler is on official business, shall be allowed only to the extent that the fee does not exceed the cost of public transportation.
- C. When a privately owned automobile is used for travel, the total transportation cost (including mileage allowance, parking fees, tolls and per diem expenses) shall not exceed the cost of public transportation, if reasonable public transportation is available.
- D. The use of rented automobiles will be kept to an absolute minimum and rented only in an emergency upon prior approval of the responsible Department Head. Every effort shall be made to obtain other suitable transportation rather than to use rented vehicles. Where emergencies require the use of a rented vehicle, the most economical vehicle available and suitable for the conduct of County business shall be obtained.

SECTION VII

LIVING EXPENSES

A. **Meals and Incidental Expense (M&IE)**

Employees assigned to out of town travel shall receive a per diem set by the current U.S. General Services Administration in their Federal Travel Regulations (FTR) Meal and Incidental Expense (M&IE) rate. Travel rates differ by travel location and are periodically revised by the Federal Government. These rates can be found at the GSA "Domestic Per Diem Rates" website page at www.gsa.gov/perdiem.

The per diem rate is intended to include all meals and incidental expenses during the period of travel. There will be no reimbursement for meals and incidental expenses beyond this rate.

In addition, the traveler may receive reimbursement for special expenses as provided in Paragraph "C-3" below.

B. **Travel Without Lodging**

When lodging is not required, the per diem M&IE allowance is not permitted. Travel shall be on "actual expenses incurred."

C. **Reimbursable Expenses**

1. Lodging - Reasonable costs of hotel accommodations incurred will be allowed. Lodging shall be reimbursed by receipt up to the limits of the current Federal Travel Regulations as shown on the GSA "Domestic Per Diem Rates" website page at www.gsa.gov/perdiem.

Questions of reasonable hotel accommodations should be referred to the Bureau of Administration. Receipts are to be submitted with the Invoice Form to support accommodation expenses claimed.

2. Transportation - Transportation to and from duty point; between places of lodging, business and meals shall be allowed.
3. Special Expenses - The reasonable cost of miscellaneous expenses incurred shall be allowed to a traveler. The following are examples of miscellaneous expenses that may be deemed reimbursable or non-reimbursable:

<u>Reimbursable</u>	<u>Non-Reimbursable</u>
Stenographic and Typing Services	Entertainment
Storage of Baggage	Alcoholic Beverages
Hire of Room for Official Business	Traffic Tickets
Telephone Calls on Official Business	

All special expenses shall be itemized on the Conference and Travel Reimbursement Voucher with receipts attached.

SECTION VIII

CONFERENCES

When the cost of meals for approved seminars or official meetings is an integral part of the Registration Fee, the "per diem" traveler shall deduct such amounts from the "cost of meals and incidental expenses" allowance, and the traveler on "actual expenses incurred" shall not claim meals which are included in the conference fee.

SECTION IX

CONFERENCE AND TRAVEL REIMBURSEMENT VOUCHER

A. Memorandum of Expenditures

A memorandum of all travel expenditures properly chargeable to the County shall be kept by individuals subject to these regulations. The information thus accumulated shall be available for proper Invoice Form preparation.

B. Conference and Travel Reimbursement Voucher Preparation

1. All claims for reimbursement of travel expenses shall be submitted on the Conference and Travel Reimbursement Voucher and shall be itemized in accordance with these regulations.
2. The Conference and Travel Reimbursement Voucher shall show the purpose of travel, the dates of travel, the points of departure and destination, mode of transportation, and the cost of the transportation secured or mileage allowance if automobile is used.
3. The Conference and Travel Reimbursement Voucher shall be supported by receipts in all instances for railroad and airplane transportation, for lodging, meals and incidental expense (M&IE) items, and all other items. Also, a copy of the travel authorization is to be included for out-of-state travel.
4. The Conference and Travel Reimbursement Voucher shall be prepared and signed by the individual who has incurred the expenses.
5. The individual submitting the Conference and Travel Reimbursement Voucher is personally responsible for accuracy and propriety. A misrepresentation shall be cause for disciplinary or legal action.

C. Approval and Submission of Invoice Form

1. The Conference and Travel Reimbursement Voucher shall be approved by the Department Head or a designated representative, who shall sign the original Voucher and submit to the Comptroller's Office. A copy of the Voucher shall be retained by the Department as well as the person submitting the Voucher.
2. Any Conference and Travel Reimbursement Voucher not prepared in accordance with these regulations or not properly supported by receipts where required will be returned to the originator for correction.

D. Frequency of Submission

The original Conference and Travel Reimbursement Voucher shall be sent to the Comptroller's Office by the 10th day of the following month in which the travel expense was incurred. Conference and Travel Reimbursement Vouchers submitted 60 days after the end of the month in which travel expense was incurred will not be reimbursed. A copy of the Conference and Travel Reimbursement Voucher shall be retained by the department and the employee.

1550-14939

EXHIBIT 8

IT Special Conditions

SEPCIAL CONDITION: FEDERAL CLAUSES

The following provisions apply to all Contracts which are funded in whole or in part with federal funds.

1. Interest of Members of or Delegates to the United States Congress

In accordance with 41 U.S.C. § 22, the Contractor agrees that it will not admit any member of or delegate to the United States Congress to any share or part of the Contract or any benefit derived therefrom.

2. False or Fraudulent Statements and Claims

(a) The Contractor recognizes that the requirements of the Program Fraud Civil Remedies Act of 1986, as amended, 49 U.S.C. §§ 3081 et seq and U.S. DOT regulations, "Program Fraud Civil Remedies," 49 C.F.R. Part 31, apply to its actions pertaining to the Contract. Accordingly, by signing the Contract, the Contractor certifies or affirms the truthfulness and accuracy of any statement it has made, it makes, or it may make pertaining to the Contract, including without limitation any invoice for its services. In addition to other penalties that may be applicable, the Contractor also acknowledges that if it makes a false, fictitious, or fraudulent claim, statement, submission, or certification, the Federal Government reserves the right to impose the penalties of the Program Fraud Civil Remedies Act of 1986, as amended, on the Contractor to the extent the Federal Government deems appropriate.

(b) The Contractor also acknowledges that if it makes a false, fictitious, or fraudulent claim, statement, submission, or certification to the County or Federal Government in connection with an urbanized area formula project financed with Federal assistance authorized by 49 U.S.C. § 5307, the Government reserves the right to impose on the Contractor the penalties of 18 U.S.C. § 1001 and 49 U.S.C. § 5307(n)(1), to the extent the Federal Government deems appropriate.

3. Federal Interest in Patents

(a) General. If any invention, improvement, or discovery of the Contractor is conceived or first actually reduced to practice in the course of or under the Contract, and that invention, improvement, or discovery is patentable under the laws of the United States of America or any foreign country, the Contractor agrees to notify County immediately and provide a detailed report.

(b) Federal Rights. Unless the Federal Government later makes a contrary determination in writing, the rights and responsibilities of the County, Contractor, and the Federal Government pertaining to that invention, improvement, or discovery will be determined in accordance with applicable Federal laws and regulations, including any waiver thereof. Unless the Federal Government later makes a contrary determination in writing, the Contractor agrees that, irrespective of its status or the status of any subcontractor at any tier (e.g., a large business, small business, non-profit organization, institution of higher education, individual), the Contractor agrees it will transmit to the Federal Government those rights due the Federal Government in any invention resulting from the contract.

4. Federal Interest in Data and Copyrights

(a) Definition. The term "subject data" used in this section means recorded information, whether or not copyrighted, that is delivered or specified to be delivered under the Contract. Examples include, but are not limited, to: computer software, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog item identifications, and related information. The term "subject data" does not include financial reports, cost analyses, and similar information incidental to Contract administration.

- (b) Federal Restrictions. The following restrictions apply to all subject data first produced in the performance of the Contract. Except as provided in the Contract and except for its own internal use, the Contractor may not publish or publicly reproduce subject data in whole or in part, or in any manner or form, nor may the Contractor authorize others to do so, without the written consent of the County and the Federal Government, until such time as the Federal Government may have either released or approved the release of such data to the public.
- (c) Federal Rights in Data and Copyrights. In accordance with subparts 34 and 36 of the Common Rule, the County and the Federal Government reserve a royalty-free, non-exclusive and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for County or Federal Government purposes, the types of subject data described below. Without the copyright owner's consent, the County and Federal Government may not extend their license to other parties.
 - (1) Any subject data developed under the contract or subagreement financed by a federal Grant Agreement or Cooperative Agreement, whether or not a copyright has been obtained; and
 - (2) Any rights of copyright which the Contractor purchases ownership with Federal assistance.
- (d) Special Federal Rights for Planning Research and Development Projects. When the Federal Government provides financial assistance for a planning, research, development, or demonstration project, its general intention is to increase public knowledge, rather than limit the benefits of the project to participants in the project. Therefore, unless the Federal Government determines otherwise, the Contractor on a planning, research, development, or demonstration project agrees that, in addition to the rights in data and copyrights set forth above, the County or Federal Government may make available to any third party either a license in the copyright to the subject data or a copy of the subject data. If the project is not completed for any reason whatsoever, all data developed under the project will become subject data and will be delivered as the County or Federal Government may direct. This subsection, however, does not apply to adaptations of automatic data processing equipment or previously existing software programs for the County's use whose costs are financed with Federal transportation funds for capital projects.
- (e) Hold Harmless. Unless prohibited by state law, upon request by the County or the Federal Government, the Contractor agrees to indemnify, save, and hold harmless the County and the Federal Government and their officers, agents, and employees acting within the scope of their official duties against any liability, including costs and expenses, resulting from any willful or intentional violation by the Contractor of proprietary rights, copyrights, or right of privacy, arising out of the publication, translation, reproduction, delivery, use, or disposition of any data furnished under the Contract. The Contractor will not be required to indemnify the County or Federal Government for any such liability arising out of the wrongful acts of employees or agents of the County or Federal Government.
- (f) Restrictions on Access to Patent Rights. Nothing contained in this section on rights in data will imply a license to the County or Federal Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the County or Federal Government under any patent.
- (g) Application on Materials Incorporated into Project. The requirements of Subsections 2, 3, and 4 of this Section do not apply to material furnished by the County and incorporated into the work.

5. Records and Audits

Contractor will deliver or cause to be delivered all documents (including but not limited to all Deliverables and supporting data, records, graphs, charts and notes) prepared by or for the County under the terms of

this Agreement to the County promptly in accordance with the time limits prescribed in this Contract, and if no time limit is specified, then upon reasonable demand therefor or upon termination or completion of the Services hereunder. In the event of the failure by the Contractor to make such delivery, then and in that event, the Contractor will pay to County reasonable damages the County may sustain by reason thereof.

The County and the Federal Government will have the right to audit all payments made to the Contractor under this Agreement. Any payments to the Contractor which exceed the amount to which the Contractor is entitled under the terms of this Agreement will be subject to set-off.

The Contractor will keep and retain records relating to this Agreement and will make such records available to representatives of the County and the Federal Government, including without limitation the sponsoring federal agency, other participating agencies, and the Comptroller General of the United States, at reasonable times during the performance of this Agreement and for at least five years after termination of this Agreement for purposes of audit, inspection, copying, transcribing and abstracting.

No provision in this Agreement granting the County or the Federal Government a right of access to records is intended to impair, limit or affect any right of access to such records which the County or the Federal Government would have had in the absence of such provisions.

6. Environmental Requirements

The Contractor recognizes that many Federal and state laws imposing environmental and resource conservation requirements may apply to the Contract. Some, but not all, of the major Federal Laws that may affect the Contract include: the National Environmental Policy Act of 1969, as amended, 42 U.S.C. §§ 4321 et seq.; the Clean Air Act, as amended, 42 U.S.C. §§ 7401 et seq. and scattered sections of 29 U.S.C.; the Clean Water Act, as amended, scattered sections of 33 U.S.C. and 12 U.S.C.; the Resource Conservation and Recovery Act, as amended, 42 U.S.C. §§ 6901 et seq.; and the Comprehensive Environmental Response, Compensation, and Liability Act, as amended, 42 U.S.C. §§ 9601 et seq. The Contractor also recognizes that U.S. EPA, U.S. DOT and other agencies of the Federal Government have issued and are expected in the future to issue regulations, guidelines, standards, orders, directives, or other requirements that may affect the Contract. Thus, the Contractor agrees to adhere to, and impose on its subcontractors, any such Federal requirements as the Federal Government may now or in the future promulgate. Listed below are requirements of particular concern.

The Contractor acknowledges that this list does not constitute the Contractor's entire obligation to meet all Federal environmental and resource conservation requirements. The Contractor will include these provisions in all subcontracts.

- (a) Environmental Protection. The Contractor agrees to comply with the applicable requirements of the National Environmental Policy Act of 1969, as amended, 42 U.S.C. §§ 4321 et seq. in accordance with Executive Order No. 12898, "Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations," 59 Fed. Reg. 7629, Feb. 16, 1994; U.S. DOT statutory requirements on environmental matters at 49 U.S.C. § 5324(b); Council on Environmental Quality regulations on compliance with the National Environmental Policy Act of 1969, as amended, 40 C.F.R. Part 1500 et seq.; and U.S. DOT regulations, "Environmental Impact and Related Procedures," 23 C.F.R. Part 771 and 49 C.F.R. Part 622.
- (b) Air Quality. The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. §§ 7401 et seq. Specifically, the Contractor agrees to comply with applicable requirements of U.S. EPA regulations, "Conformity to State of Federal Implementation Plans of Transportation Plans, Programs, and Projects Developed, Funded or Approved Under Title 23 U.S.C. or the Federal Transit Act," 40 C.F.R. Part 51, Subpart T; and "Determining Conformity of Federal Actions to State or Federal Implementation Plans," 40 C.F.R. Part 93. The Contractor further agrees to report and require each subcontractor at any tier

to report any violation of these requirements resulting from any Contract implementation activity to the County and the appropriate U.S. EPA Regional Office.

- (c) **Clean Water.** The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. §§ 1251 et seq. The Contractor further agrees to report and require each subcontractor at any tier to report any violation of these requirements resulting from any Contract implementation activity to the County and the appropriate U.S. EPA Regional Office.
- (d) **List of Violating Facilities.** The Contractor agrees that any facility to be used in the performance of the Contract or to benefit from the Contract will not be listed on the U.S. EPA List of Violating Facilities ("List"), and the Contractor will promptly notify the County if the Contractor receives any communication from the U.S. EPA that such a facility is under consideration for inclusion on the List.
- (e) **Preference for Recycled Products.** To the extent practicable and economically feasible and to the extent that it does not reduce or impair the quality of the work, the Contractor agrees to use recycled products in performance of the Contract pursuant to U.S. Environment Protection Agency (U.S. EPA) guidelines at 40 C.F.R. Parts 247-253, which implement section 6002 of the Resource Conservation and Recovery Act, as amended, 42 U.S.C. § 6962.

7. No Exclusionary or Discriminatory Specifications

Apart from inconsistent requirements imposed by Federal statute or regulations, the Contractor agrees that it will comply with the requirements of 49 U.S.C. § 5323(h)(2) by refraining from using any Federal assistance to support subcontracts procured using exclusionary or discriminatory specifications.

8. Cargo Preference - Use of United States Flag Vessels

The Contractor agrees to comply with U.S. Maritime Administration regulations, "Cargo-Preference -- U.S. Flag Vessels," 49 C.F.R. Part 381, and to include the clauses required by those regulations, modified as necessary to identify the affected parties, in each subcontract or subagreement involving equipment, materials, or commodities suitable for transport by ocean vessel.

9. Fly America

Section 14.c of the Master Agreement states that if the contract or subcontracts may involve the international transportation of goods, equipment, or personnel by air, the contract must require Contractors and subcontractors at every tier to use U.S.-flag air carriers, to the extent service by these carriers is available. 49 U.S.C. 40118 and 4 C.F.R. Part 52.

10. No Federal Government Obligations to Third Parties

The Contractor agrees that, absent the Federal Government's express written consent, the Federal Government will not be subject to any obligations or liabilities to any contractor or any other person not a party to the Grant Agreement or Cooperative Agreement between the County and the Federal Government which is a source of funds for this Contract. Notwithstanding any concurrence provided by the Federal Government in or approval of any solicitation, agreement, or contract, the Federal Government continues to have no obligations or liabilities to any party, including the Contractor.

11. Allowable Costs

Notwithstanding any compensation provision to the contrary, the Contractor's compensation under this Contract will be limited to those amounts which are allowable and allocable to the Contract in accordance

with OMB Circular A-87 and the regulations in 49 C.F.R. Part 18. To the extent that an audit reveals that the Contractor has received payment in excess of such amounts, the County may offset such excess payments against any future payments due to the Contractor and, if no future payments are due or if future payments are less than such excess, the Contractor will promptly refund the amount of the excess payments to the County.

12. Trade Restrictions

Contractor certifies that neither it nor any Subcontractor:

- (a) is owned or controlled by one or more citizens of a foreign country included in the list of countries that discriminate against U.S. firms published by the Office of the United States Trade Representative (USTR);
- (b) has knowingly entered into any contract or subcontract with a person that is a citizen or national of a foreign country on said list, nor is owned or controlled directly or indirectly by one or more citizens or nationals of a foreign country on said list;
- (c) will procure, subcontract for, or recommend any product that is produced in a foreign country on said list.

Unless the restrictions of this clause are waived by the Secretary of Transportation in accordance with 49 CFR 30.17, no Notice-to-Proceed will be issued to an entity who is unable to certify to the above. If Contractor knowingly procures or subcontracts for the supply of any product or service of a foreign country on said list for use on the project, the USDOT may direct, through the County, cancellation of the Contract at no cost to the Government.

Further, Contractor agrees that it will incorporate this provision for certification without modification in each subcontract. Contractor may rely on the certification of a prospective Subcontractor unless it has knowledge that the certification is erroneous. Contractor will provide immediate written notice to the County if it learns that its certification or that of a Subcontractor was erroneous when submitted or has become erroneous by reason of changed circumstances. Each Subcontractor must agree to provide written notice to Contractor if at any time it learns that its certification was erroneous by reason of changed circumstances. Nothing contained in the foregoing will be construed to require establishment of a system of records in order to render, in good faith, the certification required by this provision.

The knowledge and information of the Contractor is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

This certification concerns a matter within the jurisdiction of an agency of the United States of America and the making of a false, fictitious, or fraudulent certification may render the maker subject to prosecution under Title 18, United States Code, Section 100.

13. Contract Work Hours and Safety Standards Act

If applicable according to their terms, the Contractor agrees to comply and assures compliance with sections 102 and 107 of the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. §§ 327 through 333, and implementing U.S. DOL regulations, "Labor Standards Provisions Applicable to Contracts Governing Federally Financed and Assisted Construction (also Labor Standards Provisions Applicable to Nonconstruction Contracts Subject to the Contract Work Hours and Safety Standards Act)," 29 C.F.R. Part 5; and U.S. DOL regulations, "Safety and Health Regulations for Construction," 29 C.F.R. Part 1926. In addition to other requirements that may apply:

- (a) In accordance with section of the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. §§ 327 through 332, the Contractor agrees and assures that, for the Contract, the wages of every mechanic and laborer will be computed on the basis of a standard work week of 40 hours,

and that each worker will be compensated for work exceeding the standard work week at a rate of not less than 1.5 times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The Contractor agrees that determinations pertaining to these requirements will be made in accordance with applicable U.S. DOL regulations, "Labor Standards Provisions Applicable to Contracts Governing Federally Financed and Assisted Construction (also Labor Standards Provisions Applicable to Nonconstruction Contracts Subject to the Contract Work Hours and Safety Standards Act)," 29 C.F.R. Part 5.

- (b) In accordance with section 107 of the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. § 333, the contractor agrees and assures that no laborer or mechanic working on a construction contract will be required to work in surroundings or under working conditions that are unsanitary, hazardous, or dangerous to his or her health and safety, as determined in accordance with U.S. DOL regulations, "Safety and Health Regulations for Construction," 29 C.F.R. Part 1926.

14. Veteran's Preference

In the employment of labor (except in executive, administrative, and supervisory positions), preference will be given to Vietnam-era veterans and disabled veterans. However, this preference may be given only where individuals are available and qualified to perform the work to which employment relates.

15. Copyright Ownership

Consultant and the County intend that, to the extent permitted by law, the Deliverables to be produced by Consultant at the County's instance and expense pursuant to this Agreement are conclusively deemed "works made for hire" within the meaning and purview of Section 101 of the United States Copyright Act, 17 U.S.C. §101 et seq. (the "Copyright Act"), and that the County will be the copyright owner of the Deliverables and of all aspects, elements and components of them in which copyright can subsist.

To the extent that any Deliverable does not qualify as a "work made for hire," Consultant irrevocably grants, conveys, bargains, sells, assigns, transfers and delivers to the County, its successors and assigns, all right, title and interest in and to the copyrights and all U.S. and foreign copyright registrations, copyright applications and copyright renewals for them, and other intangible, intellectual property embodied in or pertaining to the Deliverables prepared for the County under this Agreement, free and clear of any liens, claims or other encumbrances, to the fullest extent permitted by law. Consultant will execute all documents and perform all acts that the County may reasonably request in order to assist the County in perfecting its rights in and to the copyrights relating to the Deliverables, at the sole expense of the County.

Consultant warrants to County, its successors and assigns, that on the date of transfer Consultant is the lawful owner of good and marketable title in and to the copyrights for the Deliverables and has the legal rights to fully assign them. Consultant further warrants that it has not assigned any copyrights nor granted any licenses, exclusive or nonexclusive, to any other party, and that it is not a party to any other agreements or subject to any other restrictions with respect to the Deliverables. Consultant warrants and represents that the Deliverables are complete and comprehensive, and the Deliverables are a work of original authorship.

16. Accessibility Compliance

If this Agreement involves design for construction, the Consultant warrants that all design documents produced or utilized under this Agreement and all construction or alterations undertaken under this Agreement will comply with all federal, state and local laws and regulations regarding accessibility standards for persons with disabilities or environmentally limited persons including, but not limited to, the following: the Americans with Disabilities Act of 1990, 42 U.S.C. § 12101 et seq. and the Americans with Disabilities Act Accessibility Guidelines for Buildings and Facilities ("ADAAG"); the Architectural Barriers Act, Pub. L. 90-480 (1968), and the Uniform Federal Accessibility Standards ("UFAS"); and the Illinois Environmental Barriers Act, 410 ILCS 25/1 et seq., and all regulations promulgated thereunder, see Illinois Administrative Code, Title 71, Chapter 1, Section 400.110. If the above standards are inconsistent, the Consultant must comply with the standard providing the greatest accessibility. Also, the Consultant must, prior to construction,

review the plans and specifications to insure compliance with the above referenced standards. If the Consultant fails to comply with the foregoing standards, the Consultant must perform again, at no expense, all services required to be re-performed as a direct or indirect result of such failure.

17. Visual Rights Act Waiver

The Consultant/Contractor waives any and all rights that may be granted or conferred under Section 106A and Section 113 of the United States Copyright Act, (17 U.S.C. § 101 et seq.) (the "Copyright Act") in any work of visual art that may be provided pursuant to this Agreement. Also, the Consultant/Contractor represents and warrants that the Consultant/Contractor has obtained a waiver of Section 106A and Section 113 of the Copyright Act as necessary from any employees and subcontractors, if any.

18. Equal Employment Opportunity

All contracts shall contain a provision requiring compliance with E.O. 11246, "Equal Employment Opportunity," as amended by E.O. 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and as supplemented by regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

19. Copeland "Anti-Kickback" Act (18 U.S.C. 874 and 40 U.S.C. 276c)

All contracts and subgrants in excess of \$2000 for construction or repair awarded by recipients and subrecipients shall include a provision for compliance with the Copeland "Anti-Kickback" Act (18 U.S.C. 874), as supplemented by Department of Labor regulations (29 CFR part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient shall be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled. The recipient shall report all suspected or reported violations to the Federal awarding agency.

20. Davis-Bacon Act, as amended (40 U.S.C. 276a to a-7)

When required by Federal program legislation, all construction contracts awarded by the recipients and subrecipients of more than \$2000 shall include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 276a to a-7) and as supplemented by Department of Labor regulations (29 CFR part 5, "Labor Standards Provisions Applicable to Contracts Governing Federally Financed and Assisted Construction").

Under this Act, contractors shall be required to pay wages to laborers and mechanics at a rate not less than the minimum wages specified in a wage determination made by the Secretary of Labor. In addition, contractors shall be required to pay wages not less than once a week. The recipient shall place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation and the award of a contract shall be conditioned upon the acceptance of the wage determination. The recipient shall report all suspected or reported violations to the Federal awarding agency.

21. Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333)

Where applicable, all contracts awarded by recipients in excess of \$2000 for construction contracts and in excess of \$2500 for other contracts that involve the employment of mechanics or laborers shall include a provision for compliance with Sections 102 and 107 of the Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333), as supplemented by Department of Labor regulations (29 CFR part 5). Under Section 102 of the Act, each contractor shall be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than 1 ½ times the basic rate of pay for all hours worked in excess of 40 hours in the work week. Section 107 of the Act is applicable to construction work and provides that no laborer or mechanic shall be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the

purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

22. Rights to Inventions Made Under a Contract or Agreement

Contracts or agreements for the performance of experimental, developmental, or research work shall provide for the rights of the Federal Government and the recipient in any resulting invention in accordance with 37 CFR part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

23. Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended

Contracts and subgrants of amounts in excess of \$100,000 shall contain a provision that requires the recipient to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251 et seq.). Violations shall be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

24. Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)

Contractors who apply or bid for an award of \$100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient.

25. Debarment and Suspension (E.O.s 12549 and 12689)

No contract shall be made to parties listed on the General Services Administration's List of Parties Excluded from Federal Procurement or Nonprocurement Programs in accordance with E.O.s 12549 and 12689, "Debarment and Suspension." This list contains the names of parties debarred, suspended, or otherwise excluded by agencies, and contractors declared ineligible under statutory or regulatory authority other than E.O. 12549. Contractors with awards that exceed the small purchase threshold shall provide the required certification regarding its exclusion status and that of its principal employees.

EXHIBIT 9

Dell Secureworks Software License and Services Agreement

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 1: Managed Security Services Integration Plus Service Description

Managed Security Services Integration Plus Service Description

This Service Description and the attached exhibits (collectively, the "Service Description") describe the Service (as defined below) being provided to you ("Customer" or "you") by the Dell entity identified in the service order ("Service Order"), executed by Customer and such Dell entity for the purchase of this Service. The Dell entity identified in the Service Order hereafter shall be collectively referred to as "Dell SecureWorks". This Service is provided in connection with the Customer's separate, signed master services agreement or security services schedule, which explicitly authorizes the sale of managed security and consulting services. In the absence of either a master services agreement or security services schedule, the Services performed under this Service Description are governed by and subject to the terms and conditions of the Dell SecureWorks Master Services Agreement, available at <http://Dell.com/Securityterms>, which is incorporated by reference in its entirety herein (the "MSA").

Service Overview

Every Managed Security Services ("MSS") installation is unique, especially in complex technology environments. The MSS Integration Plus ("MSSI+") service (the "Service") is designed to assist Customer in better integrating their MSS Service(s) into their business processes in order to obtain maximum value from the contracted MSS Service(s). The Service will be performed by one or more expert security consultant(s) assigned from Dell SecureWorks' Security and Risk Consulting ("SRC") team (each a "Security Consultant"), who will seek to quickly understand the intricacies of Customer's environment in order to optimize the integration and performance tuning of the MSS Service(s). Consultant is a subject matter expert ("SME") on all Dell SecureWorks services and is part of a team dedicated to delivering Service.

The Service components to be performed (as set forth below) are based upon the complexity and maturity of Customer's security environment and the contracted MSS services which are unique to each Customer. During the Services Term (as defined below), Customer may select one or more Service components set forth below to be performed by Dell SecureWorks. The Service components may be performed remotely from one of Dell SecureWorks' facilities and/or onsite at one of Customer's facilities, as appropriate and agreed upon by the parties. The duration of the Service is agreed upon by the parties as set forth in the Service Order (the "Service(s) Term").

Exhibit A attached hereto describes the billing method, scheduling and completion of the Service(s).

The MSSI+ Service Term is a defined period of time. The Security Consultant will use best efforts to accomplish as many MSSI+ Service components as possible during the Services Term; as such, components are determined by Customer. The Service components that can be delivered will depend upon where Customer is in their MSS implementation lifecycle and the contracted MSS services subscribed.

What Dell SecureWorks Will Do

The most common components performed by Security Consultant(s) are listed below. Dell SecureWorks and Customer will determine what Service components are best suited to be performed in order to address Customer's highest priority objectives within the Services Term.

- * MSS "SmartStart"
- * MSS Integration
- * MSS Performance Tuning
- * Deliverables for MSSI+



Depending upon the Service Components chosen to be performed, Customer's performance of its obligations as specified herein, and the time constraints of each Service component selected by Customer, the Security Consultant duties may include the following:

- * Advising Customer on current security trends, risks, and vulnerabilities.
- * Communicating with Customer's executives and Customer's security professionals.
- * Assisting Customer with strategic planning and project management for Dell SecureWorks' MSS and/or Threat Intelligence ("TI") Services.
- * Preparation of periodic and ad-hoc reports. These reports will highlight the value and enhance Customer's understanding of the MSS and TI Services.

The Security Consultant will provide Customer with brief daily reports and updates on project status via email. The Security Consultant will also provide a final summary report outlining: the work completed during this Service component, any processes that were established or agreed upon as they relate to the MSS, and recommendations for improvements to Customer's security posture. The deliverables will focus on the information most relevant to Customer, especially as it relates to Customer's business, operational, and risk-mitigation goals.

Customer Obligations

Customer agrees to perform the obligations set forth below and acknowledges and agrees that Dell SecureWorks' ability to perform the Service(s) is dependent upon Customer's compliance with the following:

- * Customer will schedule and make available all required Customer resources, including, e.g., suitable workspace and building access for Dell SecureWorks' staff and equipment, and access to Customer's computer systems and network for testing.
- * Customer will provide timely replies to all reasonable requests for documents and information in accordance with the timeframes established in the planning phase.
- * Customer's management team will support Customer's personnel being available to participate in the project plan. This is crucial to timely and successful completion of the Service(s).
- * Customer's testing windows will allow adequate time for the Security Consultant's performance of the Service(s) requested.

Limitation on the Standard Service

The Services may be performed either onsite at the Customer location defined below and/or remotely, at one or more Dell SecureWorks secure facilities. Dell SecureWorks and Customer will determine the location of the performance of the Services to be performed hereunder during the project planning with MSSSI+ Delivery Management.

In most cases, the collection of the required Customer Data will be gathered both remote and onsite, and the drafting of the Report (as defined below) and recommendations will be performed remotely.

Business Hours

- * Work will be delivered at a rate of 40 hours per week.
- * Onsite work will be performed Monday-Thursday, between 8 am – 6 pm Local time. Fridays will be performed remote to complete reports, update tickets, and other project action items.
- * Remote work will occur Monday-Friday, between 8 am – 8 pm Eastern time.
- * Work performed outside of the criteria above, as requested or required by Customer, may incur additional Service charges and requires the approval of MSSSI+ Delivery Management.



Country and Region Support

Service is offered in North America, Australia, and in English-speaking countries in Latin America and Europe. Service may be offered in other regions with the approval of MSSI+ Delivery Management prior to any binding contractual agreements being made.

Provisioning, Activation and Service Commencement

Initiation of an Engagement

Upon execution of the Service Order, the assigned Security Consultant will request certain documentation from Customer in order to review current processes, personnel, and data, in order to become familiar with Customer's organizational structure, network assets, personnel, business culture, and the maturity of Customer's security program. The Security Consultant will schedule a call ("Kick-off Call") with the Customer to discuss the engagement plan and high-level objectives. During this initial call, the parties will discuss the documentation supplied, define rules of engagement, and ensure that the scope and expectations for the Services are clearly identified and defined. See Service Scheduling below for additional details on this process.

MSS "SmartStart"

For Customers who purchase MSS SmartStart Services as indicated on a Service Order, the primary deliverables for the MSS SmartStart Service(s) component are:

- The Security Consultant will serve as the Customer's internal project manager for the MSS deployment.
- The Security Consultant will work with Customer to improve Customer's readiness to implement the MSS and deliver a strategic project plan that will present solutions to existing problems and allow quick resolution.
- The Security Consultant will make recommendations to improve Customer's security strategy and architecture, as it is relevant to the MSS deployment.
- The Security Consultant will oversee the completion of the Services Implementation Form ("SIF") on behalf of the Customer. The deliverable of this phase will be to outline the most effective approach for integrating MSS into the Customer's security environment.
- The Security Consultant will oversee the MSS Implementation from the Customer's vantage point. Successful MSS Implementations require the Customer and the Dell SecureWorks Customer Implementation Services ("CIS") team to work closely together in order to implement the MSS.
- The Security Consultant will serve as an onsite liaison between Customer's internal staff and the CIS team, to ensure deadlines and documentation requirements are being met.
- The Security Consultant will work with the Customer to successfully integrate the contracted MSS into the Customer's information security environment/program.

MSS Integration

MSS Integration assists Customer's ability to understand and more effectively consume MSS information. The Security Consultant will: (i) assist in integrating Customer data and workflows into Customer's current processes, and (ii) make recommendations for process integration and improvements in order to maximize the MSS' value for Customer.

The primary deliverables for the MSS Integration Service component are:

Reporting Setup and Customization - The Dell SecureWorks Customer Portal ("Portal") provides hundreds of pre-built security and compliance reports. The Security Consultant will provide expert guidance on which reports will best fit the needs of Customer's organization and configure all of the requirements to streamline reporting, including creation of custom reports that can be generated on demand or scheduled for recurring delivery to appropriate Customer stakeholders.

Escalation Procedures - It is critical that Customer defines its internal incident escalation procedures and provides the information to the Dell SecureWorks Security Operations Center ("SOC"). These incident escalation procedures tell the Dell SecureWorks Security Analysts when, how, and with whom to communicate within the Customer organization, in the event of a security incident. In some security environments, this process can be very simple; in more complex security environments, incident escalation procedures may vary depending on the affected asset, time of day, or type of security incident. The Security Consultant will work with Customer's team to document the incident escalation procedures that will make the most sense for Customer's organization and ensure that this information is accurately integrated into the Portal.

Asset Classification and Mapping - In order to have a clear picture of Customer's security environment, it is imperative to identify, classify, and assign criticality to each device in Customer's environment. Populating this data into the Portal enables Customer's team to report on trends by asset or asset group and to identify the potential impact of any threats, vulnerabilities, or risks associated with those assets. It also provides valuable context to the Dell SecureWorks security analysts when investigating a security event in Customer's environment, which allows the security analysts to provide more relevant and accurate alerts.

The Security Consultant will help create a plan to ensure the process of asset classification and mapping is understood, with a clear path to completion. The Security Consultant's ability to oversee the entire asset classification and mapping project will depend upon timing, the maturity of current Customer documentation and asset classification, and the ability of Customer resources to support the information required to effectively deliver this project.

MSS Performance Tuning

Continuous process improvement and optimization is a key component to the continued success of any information security program. The Security Consultant will assist Customer's security team(s) in ensuring that Customer's information security program is properly designed to get the most value from the MSS Services. The Security Consultant will work with the Customer to understand and execute on the highest-value objectives set forth in the project plan.

The primary deliverables for the Performance Tuning Service component are:

- * Improve the quality of alerts generated from the MSS by base-lining events, reviewing rule-sets and policies, and performing log analysis and optimization.
- * Filter false positives and reduce noise by tuning the MSS deployment to Customer's environment, leveraging the Dell SecureWorks SOC and Dell SecureWorks' custom tuning capabilities.
- * Act as a dedicated trusted security advisor to Customer.
- * Assist with understanding and interpreting Portal data and output from the same.
- * Understand defense-in-depth strategies and apply those to Customer's security environment as it relates to MSS.
- * Assist with integrating managed service outputs and workflows with Customer's change management processes.



- * For Customers who have purchased Dell SecureWorks' TI Service: assist with feed and Portal customization, asset profiles, and internal processes for consuming intelligence data.
- * Maintain knowledge of the Customer's information technology environment and business, attend briefings from the Dell SecureWorks counter threat unit ("CTU"), and leverage those briefings beneficially for Customer.
- * Work with Customer to develop Customer internal policies, process, and Service Level Agreements ("SLAs") (Runbook) as related to Dell SecureWorks MSS:
 - Security escalations internal to Customer, as well as outlined at Dell SecureWorks
 - Portal user access (additions/removals, permission changes/attrition, profile completion, and settings)
 - MSS device updates (additions/removals/changes)
 - Device security importance level and definition of event/incident severity, criticality, and classification
 - Incident handling (Customer incident threat level, resource handling)
 - Device tuning and management (Customer resource authority, work windows)
- * Provide information security project management assistance to Customer.
- * Work with Customer to assist with technical security escalations.
- * Keep Customer abreast of problem status, set clear expectations, provide timely follow-up to Customer, and independently handle challenging Customer situations on a daily basis.
- * Maintain knowledge of outstanding development issues and communicate development roadmap to Customer as appropriate.
- * For Customers with remaining Managed or Monitored device contract seats: provide recommendations on identifying candidates to fill seats that provide exceptional security context and awareness.
- * Conduct customized Portal training for Customer's team members.
- * Conduct customized MSS Tuning training for Customer's team members.
- * Provide reporting to Customer's designated personnel on a regular and ad-hoc basis.
- * Provide feedback for Service enhancements from Customer to Dell SecureWorks.

Deliverables for MSSI+

The Security Consultant will provide Customer with brief daily reports and updates on project status via email. The Security Consultant will also provide a final summary report outlining the work completed during this Service component, any processes that were established or agreed upon as they relate to the MSS, and recommendations for improvements to Customer's security posture. The deliverables will focus on the information most relevant to Customer, especially as it relates to Customer's business, operational, and risk mitigation goals.

Exhibit A – Terms and Conditions

Service Fees

- The fees for this Service are 100% billable upon Service Order execution.
- The Service will be delivered in a continuous manner, consistent with the assigned Security Consultant's normal business hours referenced above. For example, a three-week engagement that begins on a Monday will conclude on the third Friday thereafter. Once started, the Services shall not be suspended unless otherwise agreed to by the parties.
- Any unique needs or requirements must be conveyed by Customer and approved by MSSI+ Delivery Management during the project-planning phase.

Expenses (Out-of-Pocket)

- The fees for the Service(s) outlined in the Service Order include all incidental out-of-pocket expenses, such as report preparation and reproduction, faxes, copying, etc.
- The fees for the Service(s) outlined in the Service Order do not include out-of-pocket travel expenses, such as those related to transportation, meals, and lodging incurred in the performance of any onsite Services. Travel expenses incurred will be billed as actual expense(s) and shall be included on Customer's invoice for the Service(s).
- International projects include 8 hours of total travel time. After 8 hours, Customer will be billed at 50% of the hourly rate against total project hours. For example, an engagement which requires 16 hours of total travel will have 2 hours deducted from the total project hours.

Service Scheduling

Service requires Customer to have existing MSS services, be in the process of implementing MSS services, or be planning to do so in the near future. As such, it may be appropriate to commence Service after some or all MSS services are implemented. This may occur well after the execution of this Service Order, depending on the implementation timeline defined by the CIS Project Manager.

For new Customers who purchase Service along with other Dell SecureWorks services, MSSI+ Delivery Management will coordinate an opportune time to introduce Service into the implementation process. MSSI+ Delivery Management will meet with Customer early and advise on next steps that reflect Customer's unique needs, requirements, and expectations. In any case, new Customers will obtain a CIS Project Manager who will be aware that MSSI+ project exists and will assist in the coordination of the service.

For existing Customers who already have a fully implemented MSS, MSSI+ Delivery Management will contact Customer-designated representative within five business days after the execution of Service Order to schedule a time for the services outlined hereunder to be performed.

Customer will interface with MSSI+ Delivery Management initially, for scoping and scheduling of project. Consultant will be assigned approximately four (4) weeks prior to scheduled project start date. Once Consultant is assigned, he/she will develop project plan and schedule a kick-off call with Customer approximately three (3) weeks prior to project start date.

Services outlined within this Service Order require a minimum of four (4) weeks advance notification to schedule. Dell SecureWorks will use commercially reasonable efforts to meet Customer requests for dates and times for the delivery of Services, including performance of the Services during Customer-designated downtime windows, after business hours, meeting Customer deliverable deadlines, and other Customer scheduling requests. An email confirmation of an agreed-upon



schedule, sent by Dell SecureWorks, confirmed and returned by email by Customer, shall constitute formal acceptance of such schedule. Once scheduling of any onsite work at Customer facility has been mutually agreed to, any changes by Customer to the onsite work within two (2) weeks of the onsite work to be performed will incur a \$2,000 rescheduling fee. This rescheduling fee does not apply to work that does not require travel by Dell SecureWorks Consultant.

The designated Customer contact will receive an email from Dell SecureWorks indicating the completion of the Services, upon the earlier to occur: (i) the completion of Service(s)/Project plan, or (ii) the expiration of the Services Term. Unless Customer notifies Dell SecureWorks otherwise, in writing, within thirty (30) days of the date of such email, the Service(s)/ Project plan shall be deemed complete.

Service Order Term

The term of the Service Order and the Services shall commence on the Service Order Effective Date and terminate 12 months thereafter.

Upon completion of the Services (or each Engagement), Customer's designated contact will receive an email confirmation from Dell SecureWorks, noting the completion of the Services. Unless otherwise notified in writing to the contrary by the Customer-designated contact within thirty (30) days of such email confirmation, the Services (Engagement) shall be deemed complete.

Post Engagement Activities

Upon the "Engagement Conclusion" defined as the earlier to occur of (i) acceptance by Customer of the final Customer Report, and (ii) thirty (30) days after the delivery of the final Customer Report, Dell SecureWorks will commence with the appropriate media sanitization and/or destruction procedures of the Customer-acquired images, hard drives, or other media obtained by Dell SecureWorks in the performance of the Services hereunder (the "Incident Media"), unless, prior to such commencement, Customer has specified in writing to Dell SecureWorks any special requirements for Dell SecureWorks to return such Incident Media (at Customer's sole expense). Upon Customer's request, Dell SecureWorks will provide options for the transfer to Customer of Incident Media and the related costs thereto. If so requested, Dell SecureWorks will provide a confirmation letter to Customer, addressing completion and scope of these post-incident activities, in Dell SecureWorks' standard form. Unless agreed to otherwise by the parties and in accordance with the Record Retention section below, Dell SecureWorks shall, in its sole discretion, dispose of the Incident Media on or after the Engagement conclusion and only maintain a copy of the final Customer Report and associated deliverables.

Other Terms

Legal Proceedings

Customer shall immediately notify Dell SecureWorks if Customer knows or has reason to believe that Dell SecureWorks' Consultants, performing Services under the Service Order, have been or will be required or requested—as a result of activity arising out of or related to the Service Order or the Services contemplated hereunder, by any court or administrative agency of the United States or any other country or any state or by any legal process or party to any proceeding—to testify or to respond to any subpoena, search warrant, discovery, or other directive under the authority of such court, administrative agency, governmental inquiry, or process in connection with any proceeding or investigation in which Customer or any of its Affiliates, officers, directors, agents, employees, or subcontractors are involved. Whether or not such notice is given by Customer, Customer shall directly assist Dell SecureWorks in Dell SecureWorks' attempt to reduce the burdens of compliance with any such directive, and Customer shall reimburse any and all expenses incurred by Dell SecureWorks and its Affiliates, officers, directors, agents, employees, or subcontractors in complying with any such



directive, including, but not limited to, Dell SecureWorks' outside law firm attorneys' fees for representation and counsel, travel, lodging, and per diem expenses and an hourly labor rate at the retained hourly rate specified in the Service Order for all time spent by Dell SecureWorks in responding to such matters.

Onsite Services

Notwithstanding Dell SecureWorks' employees' placement at the Customer location, Dell SecureWorks retains the right to control the work of such employees. For international travel, onsite Services may require additional documentation, such as Visas, visitor invitations, etc., which may affect timing of the Services and reimbursable expenses.

Record Retention

Dell SecureWorks will retain a copy of the Customer Report(s) and supporting Customer Data in accordance with Dell SecureWorks' record retention policy, which provides such retention for a period commensurate with such Customer Reports' and supporting Customer Data's usefulness and Dell SecureWorks' legal and regulatory requirements and Dell SecureWorks' directives.

© 2015 Dell Inc. All rights reserved. Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Specifications are correct at date of publication but are subject to availability or change without notice at any time. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography.

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 2: Incident Management Retainer Service Description

Incident Management Retainer

Service Description

This Service Description and the attached exhibits (the "Service Description") describes the Service (as defined below) being provided to you ("Customer" or "you") by the Dell entity identified in the service order ("Service Order") executed by Customer and such Dell entity for the purchase of this Service. The Dell entity identified in the Service Order hereafter shall be collectively referred to as "Dell SecureWorks". This Service is provided in connection with Customer's separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security and consulting services. In the absence of either a master services agreement or security services schedule, the Services performed under this Service Description are governed by and subject to the terms and conditions of the Dell SecureWorks Master Services Agreement, available at <http://Dell.com/Securityterms> which is incorporated by reference in its entirety herein (the "MSA").

Service Overview

The Dell SecureWorks® Incident Management ("IM" or "Incident Management") Retainer ("IM Retainer") Services (the "Service") provides a full spectrum of use cases and capability maturity for IM that are described in this Service Description. All Services are available in the English language only.

Service Levels

Service level agreements for the Service are defined for a specific service component in the Services Scheduling section below in Exhibit A.

What Dell SecureWorks Will Do

Customer may select to apply the IM Retainer to one or more of the Service components set forth below. Upon request by Customer and upon completion of a particular Service component, Dell SecureWorks will notify Customer of the remaining IM Retainer balance. The duration of the Service is agreed upon by the parties as set forth in the Service Order Term (as defined below). Each Service component performed under this IM Retainer will vary during the Term, based upon Customer needs and availability of hours.

The Service components are summarized in the table below.

Service Option	Components
<i>Retained Incident Management Services</i>	Incident Management Briefings and Advisory
<i>Proactive Service Options</i>	<ul style="list-style-type: none"> Incident Management Workshop Incident Response Plan and Playbook Reviews Incident Response Training Workshops and Exercises Incident Response Plan and Playbook Development Compromise Screening Assessment Incident Management Risk Assessment
<i>Reactive Service Options</i>	<ul style="list-style-type: none"> Digital Forensics and Incident Response Services Emergency Incident Response Services Digital Forensic Analysis Services



	<ul style="list-style-type: none"> * Anti-Phishing Response Services * Incident Coordination Services * Cloud Incident Response Services
<i>Premium Services</i>	<ul style="list-style-type: none"> * Advanced Malware Analysis and Reverse Engineering Services * Incident Surveillance Services * Targeted Threat Hunting and Response

Report of Findings

Presentation of the findings and exact deliverables complied by Dell SecureWorks in the performance of the Services (the "Customer Report" or "Report") are tailored to the type of work performed, and to Customer's needs. The scope of the final Customer Report will be defined during the planning phase, and may include interim or ad-hoc reporting. The Customer Report will focus on the information most relevant to Customer specifically as it relates to Customer's business, operational and risk mitigation goals.

Customer Report format considerations:

- * Timing of requested Customer Report.
- * Complexity of the incident.
- * Customer updates during the analysis, even if the incident and analysis is incomplete and opinion is only provisional.
- * The complexity and sufficiency of the evidence that must be analyzed before a logically supportable opinion can be formed.
- * The audience for the Customer Report, and their requirements (for example, law enforcement, boards of directors, regulatory agencies, internal executive staff, internal IT staff, etc.).

Customer Reports may include:

- * Regular Status Reporting (written or verbal per Customer request):
 - Summary of activities completed.
 - Issues requiring attention and plans for the next work effort period.
 - Updates will initially be provided on a daily basis for active incident response Engagements; thereafter, weekly updates may be provided for extended Engagements
- * Incident response report that documents the event with the following information where possible:
 - Identifying the details of the incident in sequential order.
 - Associating a timeline with the incident.
 - Identifying any sequential or cascading components of the incident.
 - Identifying the specific attack vector used and the specific vulnerability exploited at each stage of the incident.
 - Establishing the root cause of the incident.
 - Assessment of impact.
 - Identify areas of improvement to existing information security practices.
- * Chain of custody documents.
- * Engagement findings report.
- * Incident response plan materials.



Within three (3) weeks of completing an Engagement, Dell SecureWorks will issue a draft formal Report to Customer's designated point of contact. Customer shall have three (3) weeks from delivery of such draft formal Report to provide comments concerning the nature and scope of the Engagement to be included in the final Report (the "Report Review Period"). If there are no comments received from Customer before the expiration of the Report Review Period, the Report shall be deemed final and Dell SecureWorks will finalize for distribution.

Customer Obligations

Customer acknowledges that Dell SecureWorks' ability to perform the Services hereunder is contingent upon the following:

- * Customer resources are scheduled and available.
- * For onsite Services to be performed, Customer has provided suitable workspace and necessary accesses for Dell SecureWorks' staff and equipment.
- * Access to Customer's computer systems, devices and network as necessary to perform the Services is made available to Dell SecureWorks.
- * Replies to all document requests and other information are timely and in accordance with the delivery dates established in the planning phase.
- * Customer's testing windows allow adequate time for Dell SecureWorks' performance of the Services.
- * Customer's contracted third parties involved in an Engagement will be cooperative and forthcoming with required information. Such cooperation includes but is not limited to the following:
 - Actions taken during the course of the investigation;
 - Findings reports from any other investigative firms;
 - Providing Dell SecureWorks copies of original evidence files and or images where sound forensic processes were employed.
- * Customer acknowledges that they are the best informed as to their contractual privileges and responsibilities with respect to contracted third party services such as Cloud or hosted environments and will provide Dell SecureWorks with authoritative positions regarding permissions to operate in third party environments for the purposes of this Service Order.
- * Customer accepts responsibility for obtaining any and all necessary third party authorizations required to perform services in Cloud, Hosted, Co-location or other environments not owned by Customer.

Service Assumptions

Location of Services

The Services may be performed either onsite at the Customer location defined below and/or remotely at one or more Dell SecureWorks secure facilities. Dell SecureWorks and Customer will determine the location of the performance of the Services to be performed hereunder. Note: In many cases, remote support can be used while IR personnel are in-transit to Customer's location.

Dell SecureWorks' individuals may engage in a combination of onsite and remote work effort. Other IR, Security and Risk Consulting, (SRC), Counter Threat Unit (CTU) and/or SOC analysts may work at Dell SecureWorks facilities in coordination with the primary Engagement personnel. Customer understands and acknowledges that Incident Handlers may be selected for their overall experience in handling Engagements specific to the nature of the incident as well as their availability and geographic proximity to the Customer's location(s).

Business Hours

Proactive Services

- * Onsite work will be performed Monday-Friday, 8 am – 6 pm local time.
- * Remote work may occur Monday-Friday, 8 am – 6pm local time for the assigned resource.

Reactive Services

After first understanding the nature and scope of the declared cyber incident, Dell SecureWorks will schedule available Dell SecureWorks Incident Response (IR) personnel consistent with your response goals, the specified sense of urgency, and in compliance with applicable laws or ordinances, if any.

Country and Region Support

The onsite response service level agreement (SLA) referenced in Exhibit A as "onsite response supported locations" is only available for Customer locations in the United States of America and the United Kingdom.

The in-transit response service level agreement (SLA) referenced in Exhibit A as "in-transit response supported locations" is only available for Customer locations where there are no circumstances or contingencies outside the reasonable control of Dell SecureWorks that prohibit commercially reasonable efforts for Dell SecureWorks personnel to arrive onsite.

Provisioning, Activation, and Service Commencement

Initiation of an Engagement

Once Customer initiates a request for Service through any of the predefined escalation channels, Dell SecureWorks Incident Response personnel will draft and coordinate the exchange of an "Engagement Request for Incident Management Services" document in a form substantially similar to **Exhibit B** attached hereto. For notifications made into the SOC with a request for any Services, the SOC will notify Incident Response personnel. IR personnel will make contact with the Customer via designated communication channels as soon as reasonable, but no longer than four (4) hours after being notified by the SOC. During the initial conversation, Customer and IR personnel will determine the appropriate course of action based on the estimated work effort required.

This Service provides priority access to Dell SecureWorks personnel who are available 24/7/365 via a dedicated phone-line or ticket requests to the SOC via the Dell SecureWorks customer portal ("Portal"). Preliminary direction and advice can be provided by SOC personnel. If the circumstance is deemed serious and additional expertise is desired, Dell SecureWorks IR personnel can be notified to engage with Customer personnel to conduct an in-briefing and begin assessment of the known facts. Estimated work effort required will be provided once Customer engages Dell SecureWorks IR personnel with a request for IR Service and the nature and scope of the incident is initially assessed.

Dell SecureWorks will assign no less than one incident handler ("Incident Handler") and one delivery manager ("Delivery Manager") to the Service.

Services Pre-Planning and Coordination

Upon Dell SecureWorks' receipt of a Customer executed Service Order, Dell SecureWorks will begin establishing workflows to support Customer requests for Incident Management Services. The following actions will be taken by Dell SecureWorks personnel:

- Distribute contact information to Customer for engaging with Dell SecureWorks for IR and digital forensics services. Contact information includes the 24/7/365 IR hotline, the IR Resource Coordinator and IR Delivery Managers;
- Provide Customer with artifact acquisition, chain of custody and secure transport instructions;
- Facilitate a Service initiation conference call with the Customer point of contact to review all Services available, clarify escalation channels and verify Customer contact information;
- Provision Customer access to the Portal for IR and forensics service request tickets;
- Coordinate Retained Hour utilization notifications and facilitate non-billable, on-demand meetings to scope proactive and reactive Service Engagements.

Retained Incident Management Services

Incident Management Briefings and Advisory

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, conference calls or onsite workshops can be arranged to review lessons learned from previous incidents that have occurred, to review the overall status of the Customer's Incident Management program, or provide guidance on topics of interest that fall within the domain of Incident Management.

Proactive Service Options

Incident Management Workshop

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, an onsite Dell SecureWorks consultant ("Consultant") led workshop can be arranged during the Services initiation process to review IR capability with Customer key personnel and conduct a tabletop exercise to establish IR processes for engaging with Dell SecureWorks for Incident Management Services. This optional workshop allows Dell SecureWorks to become familiar with Customer's organizational risk profile, logging and detection capabilities, IR capabilities and key personnel prior to responding to any active IR support requests. This workshop will support the creation of an information profile on the Customer's environment for Dell SecureWorks IR personnel to provide more efficient and tailored Services.

Incident Response Plan and Playbook Reviews

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks will conduct a detailed review of Customer's existing IR capabilities. Dell SecureWorks will request documentation that supports the effort to understand the Customer's current IR posture and practices in order to provide an analysis of IR capabilities based on Dell SecureWorks' breadth of experience, recommendations based on assessment of Customer's environment and relevant standards or regulatory requirements. The documentation requested will consist of items such as process diagrams, policies, procedures, guidelines and any other pertinent information to help Dell SecureWorks understand Customer's current practices and regulatory requirements. As deemed necessary, facilitated workshops and interviews may also be conducted with Customer key stakeholders to rapidly gather a deeper understanding of overall requirements, critical business requirements and existing response capabilities. It is anticipated that Customer's Engagement point of contact will provide the requested information and access to key stakeholders as rapidly as possible once the Engagement begins. At the close of the Engagement, Customer will receive a risk prioritized findings and recommendations report to improve IR practices.

Incident Response Training Workshops and Exercises

Upon, Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks will facilitate IR with specific topics customized to improve Customer's IR capabilities. Dell SecureWorks will also test Customer's IR plan with facilitated tabletop and functional exercises. Dell SecureWorks testing exercises feature tailored threat scenarios relevant to Customer's organization that are intended to proactively highlight gaps or issues with Customer's strategies and plans.

Incident Response Training Workshops

The content covered in IR Training Workshops will vary based on the maturity of existing capabilities and desired objectives. Available IR Training Workshop options may include:



- * IR fundamentals
- * Evidence handling and chain of custody
- * Volatile data collection and analysis
- * Forensic imaging techniques
- * Basic forensic analysis
- * Malware analysis for first responders

Incident Response Tabletop Exercises

An IR tabletop exercise involves assembling key IR stakeholders in a single place and walking through a scripted exercise. The facilitator releases information concerning the incident in a controlled manner that will guide the exercise, while each stakeholder describes the role they would play in a real incident. IR tabletop exercises are an efficient way to familiarize staff with IR practices and proactively test existing response plans. IR tabletop exercises are highly effective to validate roles, responsibilities, coordination and decision-making.

Incident Response Functional Exercises

Functional exercises are appropriate after tabletop IR exercises have already been performed and lessons learned from previous tabletop IR exercises have already been adopted. Functional exercises allow Customer's personnel to validate their operational readiness for incidents by performing their duties in a simulated manner. Functional exercises are designed to exercise the roles and responsibilities of specific team members and procedures in one or more functional aspects of a plan. Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.

Dell SecureWorks can coordinate overt and covert IR functional exercises.

An overt functional exercise involves the participants functionally performing each step of the plan as if it were a real incident. All participants are aware that it is an exercise, but attempt to perform actual response activities during the exercise.

A covert functional exercise is where only the Engagement point of contact or their designee is aware that the testing is an exercise. Typically only organizations that have mature response capabilities undertake covert functional exercises due to the complexity of preparing and coordinating this type of response exercise.

IR training and exercise Engagements include the following major delivery phases:

- * One Consultant will review existing IR materials and work with the Customer Engagement point of contact to verify the overall test plan and scenario injects are appropriate;
- * At least one Consultant will be scheduled for one day onsite to function as the facilitator and data collector for the exercise. For exercise groups larger than ten people, for exercises that span multiple locations, or for any functional exercises, the facilitator and data collector roles will require at least two Consultants;
- * One Consultant will provide Engagement after action reporting and follow-up support.

At the close of a training or response exercise Engagement, Customer will receive an after action report that summarizes the event activities with risk prioritized findings and recommendations to improve IR practices.

Incident Response Plan and Playbook Development

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks will assist with developing IR Plan materials at both a strategic and tactical level. At the strategic level, Dell SecureWorks will assist with IR plan development, security policy integration, capability development

and governance. From a tactical standpoint, Dell SecureWorks will help define IR workflows, roles and responsibilities, as well as detection and response procedures specific to Customer's organization.

Dell SecureWorks will request documentation that supports the effort to understand Customer's current posture and practices in order to draft IR materials tailored to Customer's organization. The documentation requested will consist of items such as process diagrams, policies, procedures, guidelines and any other pertinent information necessary to help Dell SecureWorks to understand current practices and regulatory requirements. As deemed necessary, facilitated workshops and interviews may also be conducted with Customer key stakeholders to rapidly gather a deeper understanding of overall requirements, critical business requirements and existing response capabilities. It is anticipated that Customer's Engagement point of contact will provide the requested information and access to key stakeholders as rapidly as possible once the Engagement begins.

Please note that this Engagement requires ample commitment and participation by Customer representatives by actively participating in the development process, providing information in a timely manner and reviewing drafted content to confirm the material is suitable for Customer's organization.

Dell SecureWorks will create IR Plans incorporating any previously available content that may include the following sections:

- * IR Charter
- * Delineation of Roles, Responsibilities, Dependencies and Levels of Authority for Incidents
- * Incident Categorization and Severity Definitions
- * Procedural Flows and Escalation Procedures for Incident Handling
 - Event Detection Process
 - Triage and Analysis Process
 - Incident Declaration Process
 - IR and Recovery Process
 - Incident Communication Process
- * Reporting Procedures, Templates and Forms
- * Response Team, Key Vendor and Law Enforcement Contact Information
- * Internal and External Notification Requirements
- * Employee Awareness and Readiness Training
- * Post-Incident Analysis and Improvement Process
- * IR Metrics

Compromise Screening Assessment

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks will perform compromise screening assessments that may include the analysis of log data, packet captures and forensically acquired images from key devices within Customer's infrastructure. These artifacts will be analyzed for signs indicative of compromise activity. Artifacts will be analyzed as needed, based on availability and relevance to the assessment scope and required work effort. The data from these artifacts will be screened for threat indicators using a combination of publically available and Dell SecureWorks proprietary tools and methods. These proprietary tools and methods will be used to identify patterns of behavior and communications that may indicate unknown compromise activity. Any log data should be provided to Dell SecureWorks in a clear text format that enables the application of threat intelligence. The storage size of artifacts to be analyzed will be assumed to be the actual, uncompressed volume of data when estimating level of effort.

As deemed necessary and appropriate, Dell SecureWorks may deploy live network traffic analysis appliances on Customer's network to obtain a network-centric view of live traffic with the aim of

identifying active connections to known malicious addresses, command and control servers and traffic patterns representative of malware.

To deploy these live network traffic analysis appliances, Dell SecureWorks will work with Customer's personnel to select appropriate network locations that will inspect as much "host-to-Internet" traffic as possible so that an appropriate amount of data is collected and analyzed. The live network traffic analysis appliances will only operate in detection mode and not alter or block any traffic during the Engagement.

The design and placement of the live network traffic analysis appliances will be verified in the early stages of the Engagement and may consist of one or more sensor live network traffic analysis appliances. Customer personnel must perform minor network configuration changes to accommodate network traffic analysis. Management and analysis access to the sensors live network traffic analysis appliances will be finalized during the pre-deployment phase. Dell SecureWorks will manage and operate the live network traffic analysis appliances for the duration of the Engagement.

When any compromise activity is identified, Dell SecureWorks can help plan containment and eradication or conduct post-incident forensic analysis. At the close of the assessment, Customer will receive a findings and recommendations report that includes any compromise activity observed and recommendations to improve IR practices.

Incident Management Risk Assessment

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks will conduct an operational and technical risk assessment of Customer's incident management capabilities to detect and mitigate malicious threat actors and commonly exploited threat vectors. An operational review will be conducted to assess current IR practices and measure capability maturity relative to Dell SecureWorks' breadth of experience for threat scenarios of concern. A technical review can also be performed to validate IR operational practices and identify any gaps in compromise detection capabilities. The Incident Management Risk Assessment can inform any modifications required for IR strategy, plans, playbooks and testing practices. When any compromise activity is identified during the technical review, Dell SecureWorks will help plan containment and eradication or conduct post-incident forensic analysis. At the close of the Engagement, Customer will receive a risk prioritized findings and recommendations report to improve IR practices.

Reactive Service Options

Digital Forensics and Incident Response Services

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks can provide Digital Forensics and Incident Response ("DFIR") Services. Once an incident is declared by Customer and depending on the circumstances of the incident, Dell SecureWorks can provide onsite or remote support.

In order to maintain independence during the investigation, Dell SecureWorks will not perform remediation activities. This includes the removal or cleaning of any identified malicious code or root kits, or any other similar items. Dell SecureWorks can assist in the development of remediation plans to address immediate weaknesses intended to limit the extent of the incident and minimize the potential for additional loss or damage.

Emergency Incident Response Services

Dell SecureWorks Incident Handler(s) may attempt to establish all or part of the following:

- Provide written and/or verbal guidance for Customer artifact collection.
- Provide chain of custody procedures and documentation.

- * Provide guidance and/or recommendations on remediating vulnerabilities discovered.
- * Conduct forensic analysis of hard drive(s) from Customer environment that the incident affected.
- * Conduct memory analysis of computer systems from Customer environment that the incident may have affected.
- * Conduct analysis of mobile devices from Customer's environment that the incident may have affected.
- * Conduct analysis of Credit Card end-point devices from Customer's environment that necessitate forensic review.
- * Analysis of network traffic traversing internal or external boundaries.
- * Perform custom searches based on key terms, user names, registry entries, file names, file types and/or time frame of interest.
- * Analysis of network or system log events related to the Customer incident.
- * Assessment of any recent vulnerability scans, penetration tests, web application tests, to assist in determining the unauthorized point(s) of entry.
- * Conduct analysis of open source and proprietary Threat Intelligence sources that may provide information about threats, vulnerabilities, or risks related to the incident.
- * Conduct analysis of malware or other binary files that may be involved in the incident.
- * Provide indicators of the incident and threat for use by Customer remediating the incident.
- * Provide any evidence discovered that indicates the likeness of the threat of concern.
- * Incident summary and recommendations on risk management options.
- * Provide media disposition per mutually agreed upon process. Additional costs may apply.

Digital Forensic Analysis Services

Using a variety of forensics tools and methods, Dell SecureWorks can acquire, analyze and recover data stored in the following formats:

- * Disk drives
- * Redundant Array of Inexpensive Disks (RAID) systems
- * Portable storage drives
- * Credit card skimmers
- * Mobile devices
- * Other digital media formats for analysis or data recovery

Anti-Phishing Response Services

Dell SecureWorks security analysts can analyze Phishing incidents. This can involve a variety of methodologies, depending on the nature of the incident. The objective is to gain as much information as possible about the incident to facilitate containment. A partial list of techniques includes:

- * Networking analysis techniques (traceroute, Dynamic Name System (DNS) lookups, American Registry for Internet Numbers (ARIN) searches, Operation System (OS) fingerprinting, scanning, system enumeration, foot-printing, etc.)
- * Application analysis techniques: website code reviews, email analysis, server configuration, etc.
- * Research, including Internet Relay Chat (IRC), USENET, Websites
- * Analysis of propagation methodologies and magnitudes (i.e., how is the Phishing incident being spread?).



- Severity Assessment, including analysis of the impact of the incident
- Log review—web logs, server logs, firewall logs, etc.
- Reverse lookup phone numbers used in attacks
- Notification to mobile phone Internet Service Providers (ISPs)
- Toll free reverse lookup

No commitments of Customer resources will be made without clear consent from authorized Customer personnel. With guidance and consent from Customer management where needed, Dell SecureWorks will coordinate, manage and facilitate an appropriate selection of countermeasures to have the Phishing site taken offline. These countermeasures will be selected and deployed dependent on the evolving analysis of the particular incident underway. Successful takedown is often dependent on cooperation of third parties such as internet service providers (ISPs), hosting providers, and domain registrars, among others. Dell SecureWorks does not take offensive measure to takedown phishing sites.

Incident Coordination Services

In addition to performing incident handling and digital forensic analysis Services, Dell SecureWorks can provide advisory Services in the analysis and handling of incidents. During IR, Dell SecureWorks often collaborates with executive teams, legal, public relations and other Customer key stakeholders. Dell SecureWorks' role is to provide these key stakeholders findings and impact assessments derived from IR and forensics work effort. These coordination activities may include:

- Coordinating the Engagement in-brief and regular status meetings.
- Scope definition and management during the course of the Engagement
- Engagement staff and resource management
- Engagement status reporting
- Engagement deliverable reporting
- Engagement support with the Customer and through the Customer, with other third parties

Cloud Incident Response Services

Dell SecureWorks will provide IR Services for the coordination, analysis, and handling of incidents involving the Customer Cloud Computing architecture. The Service will review evidence of compromise activity that can exist in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) Cloud Computing architectures. Dell SecureWorks IR personnel can perform investigations to determine nature and extent of suspected intrusions involving Public, Private, and Hybrid Cloud Computing architectures with the Customer and through the Customer when they are end users of Cloud Service Providers (CSPs). Cloud IR Services are highly dependent on prevailing organizational, legal, and technical factors that may complicate investigations involving the Customer Cloud Computing architecture and are conducted on a commercially reasonable effort basis.

Premium Services

In the event that Services hereunder (Premium Services) are required to assist in the delivery of any incident response services, Premium Services will be billed at 1.5 times the Retained hourly rate (Base Rate). Dell SecureWorks will not perform Premium Services work without prior customer notification, acceptance, and approval.



Advanced Malware Analysis and Reverse Engineering Services

In the event of a malicious code infection of an unknown type, Dell SecureWorks can attempt to reverse engineer the code to better understand the code's capabilities. Dell SecureWorks has extensive experience and expertise in malware reverse engineering, but this activity is conducted on a commercially reasonable effort basis because not all code can be successfully reverse-engineered. Dell SecureWorks will offer an opinion on the code's potential impact and effect on Customer assets.

Incident Surveillance Services

In an effort to ascertain additional information about the attack source and methods, Dell SecureWorks will attempt to:

- Find specific references to Customer assets affected by the current attack within underground communications.
- Identify specific references to Customer assets in attack tools or malware "kits."
- Research historic proprietary and public data regarding targeted attacks against Customer assets.
- Monitor and analyze underground communications pertaining to the active attack.

Customer will work with Dell SecureWorks to provide specific information on the assets to be covered under this project (e.g., names, identifiers, IP address ranges, brands, etc.) for correlation in counterintelligence during the active attack phase.

Targeted Threat Hunting and Response

Upon Dell SecureWorks' receipt of a Customer authorized Engagement request, Dell SecureWorks can perform a Targeted Threat Hunting and Response assessment, as set forth and described below, in the Customer environment. This service leverages Dell SecureWorks' proprietary methodology, expertise and intelligence related to advanced threat actors and their techniques, tactics and procedures (TTP). Targeted Threat Hunting and Response is specifically designed for customers that need to understand their exposure to targeted threats, and attempts to identify existing adversary presence or tradecraft in the Customer environment. The service will review evidence that may persist in network infrastructure logs, and analyze endpoint systems and other relevant data stored within the organization, to identify indicators of intrusion. When intrusions are identified, Dell SecureWorks can help plan and execute threat actor containment and eradication. At the close of the Engagement, Customer will receive a findings and recommendations report that includes any targeted threat activity observed and recommendations to improve IR practices.

The following methods may be used by the Consultants for this Engagement. These method descriptions are provided to describe the techniques that may be used, as agreed upon with the Customer. These methods are not in scope unless identified in the Scope of Work defined in the Engagement request order in a format substantially similar to **Exhibit B**, but may be added by the methods listed in the **Service Fees and Expenses** section below.

NOTE: This service requires a minimum of 150 Retained Hours.

Pre-Engagement Planning

Prior to the Engagement, the Customer will provide the assigned Dell SecureWorks team members with a completed Targeted Threat Hunting and Response Service Questionnaire and the required supporting documentation, including host and network architecture information. Dell SecureWorks will work with the customer to identify data necessary to complete the assessment and identify available sources of required data, or formulate a plan to obtain the required data. This information will be thoroughly reviewed to prepare Dell SecureWorks consultants for the Engagement.

Additional environment instrumentation (IDS/IPS, etc.) may be required to obtain the necessary data, and in these cases, Dell SecureWorks will work with the Customer to identify options they can implement prior to the Engagement. If additional instrumentation is required to effectively perform the Engagement, the project start may be delayed.

As deemed necessary and appropriate, the Engagement may commence with a workshop involving the Customer's IT security staff and the Dell SecureWorks consultants to further collect environmental specifics and calibrate Engagement objectives.

Log Assessment

The service includes the analysis of log data from key technical elements within the Customer's network. The logs will be analyzed for entries indicative of the operation of malicious software or threat actor activity. Logs will be analyzed as needed, based on availability and relevance to the assessment work.

The data from these logs will be screened for targeted threat and malware indicators using a mixture of publically available and Dell SecureWorks proprietary tools. These tools will be used to identify patterns of behavior and communications with suspicious IP addresses that may indicate the presence of malware. Due to the complexity of the search algorithms and the size of the databases behind them, some of this processing work will need to be carried out on Dell SecureWorks' owned and operated platforms.

Logs should be provided to Dell SecureWorks on disk or other storage media, or alternatively made available in a form that enables them to write code to apply intelligence to the logs. The storage size of logs to be analyzed will be assumed to be the actual, uncompressed volume when estimating the scope of work effort.

Network Traffic Analysis

As deemed necessary and appropriate, Dell SecureWorks may deploy live network traffic analysis ("Network Traffic Analysis") appliances on Customer's network to obtain a network-centric view of live traffic with the aim of identifying active connections to known malicious addresses, command and control servers, and traffic patterns that are representative of known malware.

To deploy the appliances, Dell SecureWorks will work with Customer to select appropriate network locations that will inspect as much "host-to-Internet" traffic as possible so that an appropriate amount of data is collected and analyzed. The live Network Traffic Analysis appliances will only operate in detection mode and not alter or block any traffic during the Engagement.

The design and placement of the live network traffic analysis appliances will be verified in the early stages of the Engagement and may consist of one or more sensor live network traffic analysis appliances. Customer personnel must perform minor network configuration changes to accommodate network traffic analysis. Management and analysis access to the sensors live network traffic analysis appliances will be finalized during the pre-deployment phase. Dell SecureWorks will manage and operate the live network traffic analysis appliances for the duration of the Engagement.

Endpoint Assessment – Malware Hunting

The purpose of the malware hunting portion of the Engagement is to search systems within scope for threat indicators. Based on the results, hosts will be categorized as confirmed compromised, exhibiting suspicious threat indicators or exhibiting no known threat indicators. Dell SecureWorks will conduct the following activities for the malware hunting exercise:

- Coordinate with the Customer team to execute the scans using one of several methodologies for connecting to the systems within scope.
- Run sample test scans to ensure the methodology is suitable for the target environment.



- * Scan systems for Threat Indicators using a combination of proprietary Dell SecureWorks tools, processes and intelligence.
- * Receive scan results into an agreed upon and established repository.
- * Review the scan results using threat intelligence, filter logic and established methodology.
- * Refine Threat Indicator set as necessary based on findings from initial scans.
- * Investigate any suspicious indicators/systems.
- * Working iteratively, we will repeat certain steps above, to categorize the systems according to their level of risk/suspicion.
- * Prepare findings for Customer including systems scanned, detected indicators and follow-up actions.

Containment and Response

Once sufficient evidence has been collected, the Dell SecureWorks team will help define a customized containment and eradication plan. This plan is developed in preparation for rapid execution across the organization during a specified timeframe, locking down systems and adversary access in a swift motion. This plan is also likely to include a strategy to monitor for the adversary's attempts to re-enter Customer systems. All plans and work effort will be developed with the Customer and approved by Customer prior to execution.

Exhibit A – Terms and Conditions

Service Fees

Fees for this service and the minimum hours required are defined in an associated Quote or Service Order.

Billing for the Services:

- * 100% billable upon Service Order execution
- * Retained Hours will be calculated in quarter hour increments
- * Dell SecureWorks will keep Customer informed of the balance of Customer Retained Hours
- * Hours spent delivering Premium Services are accrued and billed against the Retained Hours at a rate of 1.5 times the Retained Hourly Rate
- * Any distinction, variation, or designation of work that will be categorized as a "Premium Service" will be mutually understood and agreed upon before assignment or work is performed
- * Includes hours spent on delivering work, reporting, project management and all other work performed in this Engagement. Customer will not be invoiced for time spent traveling within an onsite response supported location.
- * Reasonable out of pocket expenses for dedicated hardware, software and shipping costs as necessary for the Engagement as well as travel, food and lodging will be invoiced separately at actual costs
- * The determination of whether Dell SecureWorks IR personnel are used for an incident will be made jointly by Customer and IR personnel during the initial contact call before any IR Services work effort is initiated
- * Any unused Retained Hours at the end of the Service Order Term will be forfeited
- * All Retained Hours are non-refundable and non-transferable for other Dell SecureWorks services
- * Additional Retained Hours must be acquired prior to the exhaustion of the Retained Hours balance for the response time commitment to remain in effect
- * This is a fixed work effort contract; not a fixed price contract. Additional blocks of hours may be retained in advance of exhaustion of contracted hours at the contracted rate by the parties by executing a change order or an additional service order for such additional hours
- * Customer may authorize continued work effort for active cyber incident response services beyond the committed hours in 40-hour increments via email to irservices@secureworks.com, to ensure continuous delivery of services. Additional hours must be authorized prior to the exhaustion of existing hours. Customer will only be billed for actual accrued hour.
- * Customer will be invoiced immediately for committed hours and monthly for additional work activity against this Service Order that are authorized via email
- * Dell SecureWorks reserves the right to bill any cyber incident declared within fourteen (14) calendar days from the Service Order Effective Date at the current Emergency Cyber Incident Response Services rate

Expenses (Out-of-Pocket)

The Service fees set forth on the Service Order include all incidental out-of-pocket expenses such as report preparation and reproduction, faxes, copying, etc.

The following out-of-pocket expenses are NOT included in the Service fees: those related to transportation, meals and lodging to travel to perform the Services. Customer agrees to reimburse Dell SecureWorks for all reasonable and actual out-of-pocket expenses incurred for travel to the Customer location in the performance of the Services. Customer acknowledges and agrees that IR by Dell SecureWorks requiring last minute air transportation will result in much higher costs than ordinary business travel as a result of the requirement to purchase tickets with little if any advance notice. Forensic work MAY also require additional costs associated with required media storage, specific equipment or licensing, depending on the size of the incident, image acquisition needs or the complexity of the incident. Such expenses will be added, at cost, to Customer's invoice.

Service Scheduling

Scheduling of Proactive Services

Proactive Services outlined above require a minimum of four (4) weeks advance notification in order to schedule. This allows Dell SecureWorks to schedule the appropriate resources to meet the specific Engagement requirements and ensure completion of the Engagement before the expiration of the Service Order Term. The Dell SecureWorks IR Resource Coordinator is available to facilitate non-billable, on-demand meetings with IR personnel to scope Proactive Services Engagements.

Scheduling of Reactive Services

Customer has 24/7/365 access to Dell SecureWorks SOC personnel and the Portal for the initial communication channel. Additional communication channels include the email addresses and phone numbers of the Dell SecureWorks IR Resource Coordinator and Delivery Managers.

Events Requiring Onsite Incident Handling (Within scope for Onsite Response Supported Locations)

Dell SecureWorks shall use commercially reasonable efforts to have an incident handler arrive onsite (i.e., "onsite presence"), within thirty-six (36) hours for onsite response supported location travel after the mutual determination by Customer and IR personnel that onsite IR is required.

Events Requiring Onsite Incident Handling (Within scope for In-Transit Response Supported Locations)

In the case that visa and work permits are not required for travel to the location in question, Dell SecureWorks shall use commercially reasonable efforts to have an incident handler board a plane or other appropriate form of transportation within forty-eight (48) hours for in-transit response supported location travel after the mutual determination by Customer and IR personnel that on site IR is required.

Customer acknowledges and agrees that it is impossible and unrealistic for Dell SecureWorks to anticipate every contingency in connection with emergency on site IR and, notwithstanding its commercially reasonable efforts, that there may be unforeseen circumstances or contingencies outside the reasonable control of Dell SecureWorks that could make compliance with the foregoing unrealistic or impossible, regardless of cost, including but not limited to: holidays, acts of war or terrorism, weather, flight availability, visa and passport requirements, restrictions of importation of encrypted technologies, handler schedules, unanticipated levels of contemporaneous emergency incident responses and other similar or dissimilar circumstances or events.



Service Order Term

The term of this Service Order shall commence on the Service Order Effective Date and terminate on the earlier to occur of (i) the date which is one (1) year thereafter, or (ii) the completion of the Services (the "Service Order Term").

The term of the Services for the Incident Management Retainer shall commence on the Service Order Effective Date and terminate on the earlier to occur of (i) the Service Order Term, or (ii) upon exhaustion of the original Retained Hours (or subsequent change order) and completion of any outstanding time and materials billing (the "Services Term").

Upon completion of the Services, the Customer designated contact will receive an email confirmation from Dell SecureWorks. Unless otherwise notified in writing to the contrary by the Customer designated contact within thirty (30) days of such email confirmation, the Services and this SOW shall be deemed complete.

Post Engagement Activities

Upon the "Engagement Conclusion" defined as the earlier to occur of (i) acceptance by Customer of the final Customer Report, and (ii) thirty (30) days after the delivery of the final Customer Report, Dell SecureWorks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Dell SecureWorks in the performance of the Services hereunder (the "Incident Media"), unless prior to such commencement, Customer has specified in writing to Dell SecureWorks any special requirements for Dell SecureWorks to return such Incident Media (at Customer's sole expense). Upon Customer's request, Dell SecureWorks will provide options for the transfer to Customer of Incident Media and the related costs thereto. If so requested, Dell SecureWorks will provide a confirmation letter to Customer addressing completion and scope of these post incident activities, in Dell SecureWorks' standard form. Unless agreed to otherwise by the parties and in accordance with the Record Retention section below, Dell SecureWorks shall, in its sole discretion, dispose of the Incident Media on or after the Engagement conclusion and only maintain a copy of the final Customer Report and associated deliverables.

Other Terms

Legal Proceedings

If Customer knows or has reason to believe that SecureWorks or its employees performing Services under this Service Order have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require SecureWorks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify SecureWorks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse SecureWorks for (a) its employees' time spent as to such response at the hourly rate reflected in this Service Order, (b) its reasonable and actual attorney's fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and SecureWorks as to the Services or this Service Order.

Onsite Services

Notwithstanding Dell SecureWorks' employees' placement at the Customer location, Dell SecureWorks retains the right to control the work of such employees. For international travel, onsite

Services may require additional documentation, such as visas, visitor invitations, etc. which may affect timing of the Services and reimbursable expenses.

Endpoint Assessment – Malware Hunting

Unless otherwise agreed upon in writing, within thirty (30) days following the expiration or termination of the Service Order (the "Thirty Day Period"), Customer shall uninstall any and all copies of the software agent used for Malware Hunting. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Dell SecureWorks' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Dell SecureWorks from the software agent. Customer will uninstall the software agent as described in the Service Order.

Record Retention

Dell SecureWorks will retain a copy of the Customer Report(s) and supporting Customer Data in accordance with Dell SecureWorks' record retention policy, which provides such retention for a period commensurate with such Customer Reports' and supporting Customer Data's usefulness and Dell SecureWorks' legal and regulatory requirements and Dell SecureWorks' directives.

Payment Card Industry Forensic Investigator Services

The PCI Forensic Investigator Services provided by Dell SecureWorks are governed by and subject to the terms and conditions of the PCI Forensic Investigator (PFI) Program Guide available at https://www.pcisecuritystandards.org/documents/PFI_Program_Guide_2.1.pdf.

Customer understands and agrees that PFI reports produced by Dell SecureWorks will not be accepted by the PCI SSC or the affected Participating Payment Brands as authorized PFI reports under the following circumstances:

- * If Dell SecureWorks (or any then-current Dell SecureWorks employee) has performed a Qualified Security Assessor ("QSA") or Approved Scanning Vendor ("ASV") Assessment within the then preceding three (3) years for the Customer.
- * If Dell SecureWorks has performed a Payment Application Qualified Security Assessor ("PA-QSA") Assessment of a payment application that is involved in a given security Issue and Dell SecureWorks is unable to ensure that the business unit and personnel utilized by such PFI Investigation in connection with such PA-QSA Assessment are reasonably separate and isolated from, and do not interfere with the independence or decision-making of, the business unit and personnel utilized by Dell SecureWorks in connection with the PFI Investigation.
- * If the Customer is using any products or services provided by or through Dell SecureWorks, other than the PFI Investigation services.

In the event that the Customer elects to have Dell SecureWorks perform Incident Response services when it is evident that Dell SecureWorks is not authorized to perform PFI Investigation services, the parties understand and agree that the PFI Investigation (i) is solely for Customer's internal purposes, (ii) does not constitute an investigation that will be recognized or accepted as a PFI Investigation by the PCI SSC or the affected Participating Payment Brands, (iii) and should not be represented as an authorized PFI Investigation to outside parties. Customer understands and agrees that if the Customer is required to undergo a PFI Investigation, Customer must engage a separate approved PFI



company to do so or seek written approval from each affected Participating Payment Brand and the PCI SSC that Dell SecureWorks is authorized to perform a PFI Investigation.

In the event Dell SecureWorks is authorized by the PCI SSC, the affected Participating Payment Brands, and the Customer to perform PFI Investigation services:

- * Customer understands and agrees that Dell SecureWorks has complete discretion to perform the PFI Investigation services in its independent, professional judgment without Customer influence, and further that a PFI Investigation is not and shall not be directed or controlled in any way by the Customer.
- * Customer understands and agrees that a "PFI Preliminary Incident Response Report" must be delivered to each affected Participating Payment Brand, and such Customer's affected acquirer(s) (if the Customer is a merchant), in each case no later than five (5) business days after beginning the PFI Investigation review.
- * Customer understands and agrees that a "PFI Final Incident Report" must be delivered to each affected Participating Payment Brand, and such Customer's affected acquirer(s) (if the Customer is a merchant), in each case no later than ten (10) business days after completion of the PFI Investigation review.
- * Customer understands and agrees that Dell SecureWorks is authorized by the requirements of the PCI PFI Program to deliver copies of the PFI Investigation reports at the same time and without any prior authorization required from the Customer to each affected Participating Payment Brand, the Customer's affected acquirer(s) (if the Customer is a merchant), and the Customer.
- * Customer understands and agrees that accounts (Credit Card Numbers/PAN's) discovered during the PFI Investigation must be uploaded to the affected Participating Payment Brands' fraud detection personnel, if applicable.

Exhibit B: SAMPLE Engagement Request for Incident Management Services

This Engagement Request documents the Incident Management Services requested by Customer that will be provided by Dell SecureWorks as a part of the Incident Management Services Service Description entered into between Dell SecureWorks and Customer. This Engagement Request will be drafted by Dell SecureWorks IR personnel when a request for an Engagement is initiated by Customer through any of the defined escalation channels. Dell SecureWorks IR personnel will distribute this form to Customer via email for review and authorization to trigger Retained Hour utilization and commencement of the Engagement. This Engagement Request must be returned by an authorized representative of Customer via email prior to commencement of the Engagement set forth below.

- 1) Engagement Code Name:
- 2) Engagement Contact Information:

Customer	
Engagement Address	
Point of Contact Name	
Point of Contact Email Address	
Point of Contact Primary Telephone Number	
Point of Contact Secondary Telephone Number	

Dell SecureWorks	
Primary Consultant Name	
Primary Consultant Email Address	
Primary Consultant Telephone Number	
Delivery Manager Name	
Delivery Manager Email Address	
Delivery Manager Telephone Number	
Practice Director Name	
Practice Director Email Address	
Practice Director Telephone Number	

- 3) Engagement Schedule:

The Incident Management Services to be rendered hereunder shall commence on <MM/DD/YYYY> and are estimated be completed no later than <MM/DD/YYYY>.

- 4) Incident Management Services Scope of Work:
- 5) Incident Management Services Deliverables:
- 6) Incident Management Services Billable Retainer Hours Estimate*:
- 7) Customer Responsibilities:
- 8) Estimated Timeline for Requested Incident Management Services:

Time Interval	Work Effort
Week 1	
Week 2	
Week 3	
Week 4	

* The Retained Hours necessary for the completion of an Engagement may vary depending on the Customer requests and the complexity of the circumstances for such Service chosen.

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 3: Counter Threat Unit™ Threat Intelligence Service Description and Service Level Agreement



Counter Threat Unit™ Threat Intelligence Service Description and Service Level Agreement

This Service Description and Service Level Agreement and the attached appendices (collectively, the "Service Description") describes the Service (as defined below) being provided to you ("Customer" or "you") by the Dell entity identified in the service order ("Service Order") executed by Customer and such Dell entity for the purchase of this Service. The Dell entity identified in the Service Order hereafter shall be collectively referred to as "Dell SecureWorks". This Service is provided in connection with Customer's signed Service Order and separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security services. In the absence of either a master services agreement or security services schedule, the Services performed under this Service Description are governed by and subject to the terms and conditions of the Dell SecureWorks Master Services Agreement, available at <http://Dell.com/Securityterms> which is incorporated by reference in its entirety herein (the "MSA").

Service Overview

Leveraging Dell SecureWorks' in-depth analysis of emerging threats and zero-day vulnerabilities, the Counter Threat Unit ("CTU") Threat Intelligence ("TI") Service (the "Service") is designed to deliver early warnings and actionable Threat Intelligence, enabling enterprises of all sizes to quickly protect against cyber threats and vulnerabilities.

Definitions

The following definitions shall have the meanings set forth below:

- **Advisories** – High-criticality threat write ups.
- **AttackerDB** – A database of known malicious attackers determined by analyzing Dell SecureWorks' security device data.
- **Attack** – Any malicious attempt to: (i) subvert, (ii) gain control, or (iii) otherwise cause damage to Customer's network or network equipment.
- **Counter Threat Unit ("CTU") research team** – Dell SecureWorks' staff who are dedicated to support the Service.
- **CTU TI Data** – All data provided to Customers as part of the Dell SecureWorks CTU Service, including but not limited to, Vulnerabilities, Advisories, and Threats.
- **Cyber Security Index (CSI)** – A threat-based, color-coded system provided to notify Customer regarding Threats that might require protective measures. The CSI is evaluated daily by CTU researchers and updated when necessary.
- **Malware** – Software developed with a malicious intent, including, but not limited to, trojans, viruses, and rootkits.
- **Normal Business Hours** – 8:30 a.m. 5:30 p.m. Eastern Standard Time.
- **Dell SecureWorks Customer Portal ("Portal")** – A secure, web-based method used by Customer to co-monitor it's environment, generate security reports, update escalation procedures, and make help desk requests.
- **Threat** – Any technique or software used to exploit Vulnerabilities.

- **Vulnerability** – A software flaw that may be exploited to allow a malicious user or code to subvert the software or host operating system.

Service Offerings Component Descriptions

Service Offerings Available with all TI Purchases Include:

Vulnerability Data Service
Threat Data Service
Advisory Data Service

Vulnerability Data Service

Dell SecureWorks' Vulnerability Data Service provides Customer with detailed descriptions and analysis of current Vulnerabilities. Vulnerabilities are processed from a number of public and private data feeds, enriched by Dell SecureWorks' CTU researchers, and reported in the Portal. Customers can customize the feed to their individual network using asset and application mapping.

Vulnerability Data Service Components include:

- Comprehensive Vulnerability Data Alerts with expert analysis;
- Threat-level evaluation of each Vulnerability;
- Customized to the Customer's network environment.

Vulnerability Data Service Example

Vulnerability Detail

Apple QuickTime Movie File 'tfto' Element Handling Byte Swapping Vulnerability

Vuln ID: 113329
URL: <https://portal.secureworks.com/intel/mva?Task=ShowVuln&VulnId=113329>
Release Date: 26 Feb 2014
Impact: Medium
CVSS Score: 5.0

A vulnerability exists in Apple QuickTime due to an out-of-bounds byte swapping error when handling crafted movie files. A remote attacker could exploit this vulnerability to cause a denial of service condition or execute arbitrary code on vulnerable systems.

Technical Analysis

Apple QuickTime is a multimedia player that supports the playback of various video, audio, and image content formats. A vulnerability exists in QuickTime versions prior to 7.7.5 for Windows and in QuickTime for Mac OS X versions 10.7.5, 10.8.5, 10.9, and 10.9.1 due to improper bounds checking. Playing a movie file containing a specially crafted 'tfto' element may trigger an out-of-bounds byte swapping error. Remote attackers could leverage this issue to crash the application or execute arbitrary code on vulnerable systems.

Solution

The vendor has released updates version to address this vulnerability. Windows users should upgrade to Apple QuickTime version 7.7.5, which can be downloaded from <https://www.apple.com/quicktime/download/>. Apple users should upgrade to Apple OS X version 10.9.2 or apply Security Update 2014-001, which can be downloaded from <http://www.apple.com/support/downloads/>.

References

1. <https://www.apple.com/quicktime/>
2. <http://www.apple.com/support/downloads/>
3. <http://www.apple.com/>
4. <http://www.apple.com/osx/>
5. <http://support.apple.com/kb/HT6150>
6. <http://support.apple.com/kb/HT6151>
7. <https://www.apple.com/quicktime/download/>
8. <http://securitytracker.com/id?1029823>
9. <http://www.securityfocus.com/bid/65777>
10. <http://xforce.iss.net/xforce/xfdb/91404>

Modification History

Revision 2 Entered on February 27, 2014

Affected Products

- Apple QuickTime (Apple/AppleQuickTime)
- Apple Mac OS X 10.7.5 (Apple/AppleMacOSX1075)
- Apple Mac OS X Server 10.7.5 (Apple/AppleMacOSXServer1075)
- Apple Mac OS X 10.8.5 (Apple/AppleMacOSX1085)
- Apple Mac OS X 10.9 (Apple/AppleMacOSX109)
- Apple Mac OS X 10.9.1 (Macintosh) (Apple/AppleMacOSX1091)

CVE Details

CVE-2014-1230

CWE Details

CWE-20: The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program.

Associated Vulnerabilities

None

Associated Threats

None

CVSS v2 Scores and Vectors

- Base Score: 5.0 (AV:N/AC:M/Au:N/C:P/D:N/I:A/P)
- Temporal Score: 5.0 (E:U/RL:O/C:C)

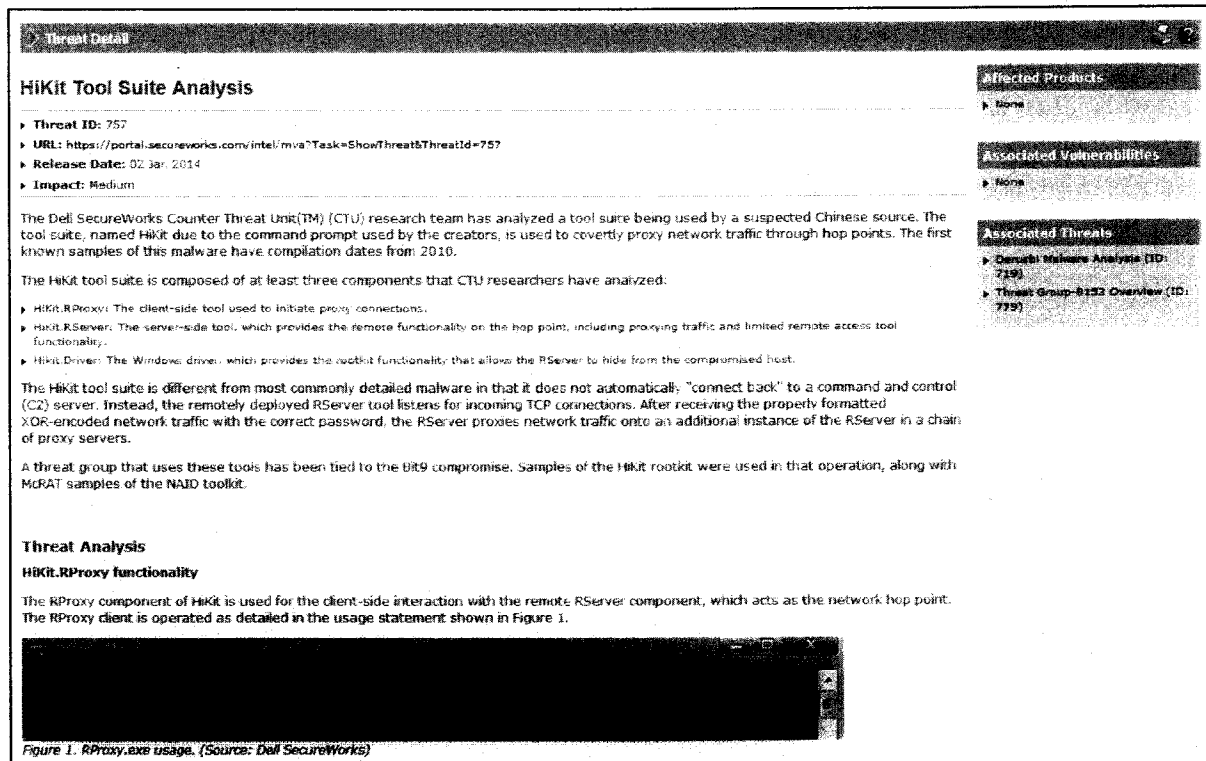
Threat Data Service

Dell SecureWorks' CTU research team will publish detailed decompositions of current Malware or Threats twice monthly. Often a Threat is a representative sample of Malware code that is selected and decomposed in a detailed Malware report.

Threat Data Service Components include:

- Detailed technical analysis illustrates popular hacker attack vectors and techniques;
- Threats are cross-referenced to pertinent Vulnerabilities.

Threat Data Service Example



Threat Detail

HiKit Tool Suite Analysis

▶ Threat ID: 757
 ▶ URL: <https://portal.secureworks.com/intel/mva?Task=ShowThreat&ThreatId=757>
 ▶ Release Date: 02 Jan 2014
 ▶ Impact: Medium

The Dell SecureWorks Counter Threat Unit(TM) (CTU) research team has analyzed a tool suite being used by a suspected Chinese source. The tool suite, named HiKit due to the command prompt used by the creators, is used to covertly proxy network traffic through hop points. The first known samples of this malware have compilation dates from 2010.

The HiKit tool suite is composed of at least three components that CTU researchers have analyzed:

- ▶ HiKit.RProxy: The client-side tool used to initiate proxy connections.
- ▶ HiKit.RServer: The server-side tool, which provides the remote functionality on the hop point, including proxying traffic and limited remote access tool functionality.
- ▶ HiKit.Driver: The Windows driver, which provides the rootkit functionality that allows the RServer to hide from the compromised host.

The HiKit tool suite is different from most commonly detailed malware in that it does not automatically "connect back" to a command and control (C2) server. Instead, the remotely deployed RServer tool listens for incoming TCP connections. After receiving the properly formatted XOR-encoded network traffic with the correct password, the RServer proxies network traffic onto an additional instance of the RServer in a chain of proxy servers.

A threat group that uses these tools has been tied to the Bit9 compromise. Samples of the HiKit rootkit were used in that operation, along with McRAT samples of the NAID toolkit.

Threat Analysis

HiKit.RProxy functionality

The RProxy component of HiKit is used for the client-side interaction with the remote RServer component, which acts as the network hop point. The RProxy client is operated as detailed in the usage statement shown in Figure 1.




Figure 1. RProxy.exe usage, (Source: Dell SecureWorks)

Affected Products

▶ None

Associated Vulnerabilities

▶ None

Associated Threats

▶ Detailed Malware Analysis (ID: 757)

▶ Threat Group-Bit9 Overview (ID: 775)

Advisory Data Service

Advisory reports contain strategic security information regarding the current Threat landscape. Typically, these reports are published once a month and include analysis of Attack data across Dell SecureWorks' monitored security devices.

Advisory Data Service components include:

- Advisories are strategic security reports pertinent to the current security landscape.
- Example topics include:
 - Threats we see targeting many of our customers;
 - High profile threats (Clampi, Conficker, etc); and
 - High-criticality threats (Internet Explorer 0-day etc.).

Advisory Data Service Example

Advisory Detail

Dell SecureWorks Security Advisory - Security Implications of Microsoft Windows XP End of Support - Action Recommended

Advisory ID: 239
URL: <https://portal.secureworks.com/intel/mva?Task=ShowAdvisory&AdvisoryId=239>
Release Date: 18 Dec 2013

Associated Vulnerabilities

None

Associated Threats

Security Implications of Microsoft Windows XP End of Support (ID: 749)

Summary

Dear Dell SecureWorks Client,

Microsoft has announced that extended support for the Windows XP operating system is scheduled to end on April 8, 2014. According to Microsoft, end-of-life for extended support means an end to the following features:

- Security updates
- Non-security hotfixes
- Free or paid assisted support options
- Online technical content updates

Recommended Actions:
The Dell SecureWorks Counter Threat Unit(CTU) research team recommends that clients migrate to a supported operating system well in advance of the April 8, 2014 end-of-support date.

Dell SecureWorks Actions:
CTU researchers have published an analysis of this issue on the public website at <http://www.secureworks.com/cyber-threat-intelligence/threats/security-implications-of-microsoft-windows-xp-end-of-support/>.

Questions:
If you have any questions or concerns, please submit a ticket via the Dell SecureWorks Customer Portal.

References:
<http://www.secureworks.com/cyber-threat-intelligence/threats/security-implications-of-microsoft-windows-xp-end-of-support/>
<http://windows.microsoft.com/en-us/windows/lifecycle>
<http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx>
<http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomid=0>
<http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx>

Service Offerings Available with Standard+, Advanced & Enterprise TI Service Purchases Include:

- Microsoft Update Summary.
- Monthly Security Intelligence Webinar.
- Emerging Threat Bulletins (CTU TIPS).
- Weekly Intelligence Summary.

Microsoft Update Summary

Within one (1) business day following a Microsoft security patch release, Customer will receive a summary security report from the CTU research team outlining the contents of the Microsoft patch. Typically, these patches occur once a month on Tuesdays.

Microsoft Update Summary service components include:

- Provided within one (1) business day of a critical Microsoft operating system patch.
- Summarizes all Vulnerabilities including a level of criticality for the overall patch.

Monthly Security Intelligence Webinar

On a monthly basis, the CTU research team will host a security briefing describing current security Threats and Advisories. This call is open to all CTU Services customers.

Webinar includes topics regarding:

- Threat webinar hosted by Dell SecureWorks CTU researchers.


- Review of current security concerns and hacker activities.

Emerging Threat Bulletins (CTU TIPS)

The CTU research team will provide real-time, emerging threat updates to TI Service customers. Customer will typically receive five (5) updates per week via email. Updates include CTU researchers' comments on emerging Threats under investigation, opinions on cyber-attack news, and updates on security concerns currently being investigated by the CTU research team.

- Bulletin data is delivered via email and provides insight into current security topics under the CTU research teams' scrutiny.
 - Topics are often unverified and may not result in a security Advisory or Vulnerability posting.
 - Bulletins are designed to keep the Customer abreast of security issues in real time.

Emerging Threat Bulletins Example

Open Sources Intelligence Update for February 21, 2014
 Feb 21, 2014
 The Dell SecureWorks CTU(TM) research team welcomes you to the Open Sources Intelligence Update for February 21, 2014. This update provides a brief daily highlight of CTU activities, major issues, and trends affecting Dell SecureWorks clients.
CTU Research
 CTU TIPS: Adobe Flash player vulnerability (CVE-2014-0502) exploited via strategic web compromises
<https://portal.secureworks.com/intel/tips/3119>
 CTU TIPS: Invitation to view CTU monthly webcast for February 2014
<https://portal.secureworks.com/intel/tips/3115>
 CTU TIPS: Update to CVE-2014-0322 - Microsoft releases Fix it tool
<https://portal.secureworks.com/intel/tips/3113>
Vulnerabilities and Threats
 Emergency Adobe Flash Update Handles Zero Day Under Attack
<http://threatpost.com/emergency-adobe-flash-update-handles-zero-day-under-attack/104387>
 Netgear quietly patches critical authentication bypass
<http://www.triowire.com/state-of-security/vulnerability-management/netgear-quietly-patches-critical-authentication-bypass/>
 Hackers moving to Android's chargeware to avoid Google and network watchdogs
<http://www.v3.co.uk/v3-uk/news/2329996/hackers-moving-to-androids-grey-area-to-avoid-google-and-network-watchdogs>
Cyber Incidents and Cyber Crime
Government, Law, and Critical Infrastructure
 S. Korea Seeks Cyber Weapons to Target North Korea's Nukes
<http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/>
 Office 365 Message Encryption - now rolling out
<http://blogs.office.com/2014/02/19/office-365-message-encryption-now-rolling-out/>
Security Industry Tools and Reports
 TIPS - a Threat Intelligence Service from Dell SecureWorks® CTU™
 CTU Cyber Security Index:
GUARDED
 Level 1
 2014-02-21 14:20:01 UTC

Weekly Intelligence Summary

On a weekly basis, a PDF report outlining the last seven (7) days of Threats, Vulnerabilities, and Advisories will be provided to TI customers via the Portal. This report also contains the daily CTU Cyber Security Index across the entire week.

- Provided every Monday via email;

November 17, 2014

Dell SecureWorks Limited External Distribution

Page 6 of 14

- Summary reports contain a breakdown of Vulnerabilities identified over the last week and a review of emerging Threat bulletins.
- Alert summary data from more than 30,000 monitored security devices is included when pertinent.

Weekly Intelligence Summary Example

Weekly Intelligence Summary

February 15 – February 21, 2014

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

The Dell SecureWorks Counter Threat Unit™ (CTU) research team welcomes you to this report summarizing the threats, vulnerabilities, malicious activity, and CTU advisories for the previous week. This report also reviews the daily CTU Cyber Security Index (CSI) threat score for the reporting period.

Client Advisories

Client advisories convey Dell SecureWorks' notification and advice on issues of significant risk, about which all enterprises should be informed.

The CTU research team published no client advisories this period.

The CSI began at Elevated (Level 2) and was downgraded to Guarded (Level 1) on Monday, February 17, 2014. CTU researchers are monitoring targeted attack activity exploiting recently disclosed vulnerabilities in Internet Explorer and Flash Player. Clients should remain vigilant for anomalous activity and apply available security updates or mitigations as soon as possible.

Dell SecureWorks SOC's noted threat activity for the following security issues (in order of reported appearance):

Service Offerings Available with Enterprise TI Service Includes:


Microsoft Update Analysis

Bi-Weekly Cyber Security Roundup

Microsoft Update Analysis

Within one (1) business day following a Microsoft security patch release, Customer will receive a detailed security report from the CTU research team outlining the contents of the Microsoft patch. Typically, these patches occur once a month on Tuesdays and the security report is provided within one (1) business day of a critical Microsoft operating system patch and Details all Vulnerabilities including a level of criticality for the overall patch.

MS Update Analysis Example


Dell SecureWorks

CTU™ Microsoft Update Analysis, January 2014

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Bulletins: 4 • CVEs: 6

Executive summary

Microsoft's monthly patch cycle for January includes 4 bulletins for a total of 6 CVEs (Common Vulnerabilities and Exposures), an open standard for cataloging computer security issues.

- Five of the covered CVEs have a Microsoft **Exploitability Index (EI)** assessment of 1 for affected software releases, making these issues attractive targets for attackers and high priorities for updating if applicable in your environment.
- Four of the covered CVEs have a lower Microsoft **Exploitability Index (EI)** assessment for the latest software release, encouraging clients to update software when appropriate.
- One of the covered CVEs has been publicly disclosed, and Microsoft is aware of limited attacks attempting to exploit the

The most important update in January is MS14-002 which addresses a zero-day vulnerability in the **NDPROXY driver (CVE-2013-5066)** from November 2013. The vulnerability has been under exploitation since November and has been distributing malware using a malicious PDF file.

Another important update this month addresses memory corruption vulnerabilities in Microsoft Word and Microsoft Office that allow for code execution via a maliciously crafted Word document. These vulnerabilities are likely to be attractive to attackers interested in phishing campaigns.

Please refer to the end of this document for a **Legend** and explanation of the various discussion sections, as well as a discussion of the different security and exploitability indexes (Xis).

The CTU research team recommends prioritizing the security updates as listed in the following chart with the most important

Bi-Weekly Cyber Security Roundup

On a bi-monthly basis, a report highlighting the last two weeks of major issues and trends as determined by Dell SecureWorks' CTU research analysts will be made available to customers via the Portal.

The report:

- will highlight stories from public news sources with a focus on issues impacting critical infrastructure sectors; and
- will be published within one (1) business day after the 1st and 15th of each month.

Add-on Service Offerings to Advanced and Enterprise TI Service Purchases Includes (add-on Services Offerings are subject to an additional fee):

Threat Intelligence Support

Attacker Database Data Feed

Borderless Threat Monitoring

Threat Intelligence Support

The TI Support Service provides customers with direct CTU research team escalation support to complement our Advanced and Enterprise Threat Intelligence Service subscriptions. TI Support Service customers can escalate TI questions / issues for enrichment directly to the CTU research team via the Portal ticketing system. This request-driven, transactional Service enables our Advanced and Enterprise TI customers to leverage the expertise and threat visibility of the CTU research team for:

- Questions / issues / clarification on TI information received via our Advanced or Enterprise TI Services and associated add-on Services including AttackerDB and Borderless Threat Monitoring.
- Transactional requests for CTU researchers to add enriched context to Customer provided threat indicators, threat context, malware samples, or TI sourced from internal Customer operations or third-party sources.

Attacker Database Data Feed

Dell SecureWorks correlates Attacks across thousands of monitored security devices on a daily basis. These Attacks are processed into an Attacker Database. A data feed of the Attacker Database ("AttackerDB") is provided to TI Services customers. The Attacker Database is updated on a daily basis.

- The AttackerDB contains lists of malicious internet protocol ("IP") addresses and domains identified by the Dell SecureWorks' managed security service business and CTU research analysts.

Attacker Database XML Export

The token provided in this section provides access to the Attacker Database XML feed. Generating a new token will revoke previous tokens. The XML export is designed for consumption by your internal systems. Use the selection boxes to automatically build the URL or manually construct it by using the listed parameters.
Note: The AttackerDB in XML format may be too large for most browsers to display. To download the AttackerDB to use in a program such as Microsoft Excel use the export as files option below.

Type: ☒ IP ☐ Domain Name

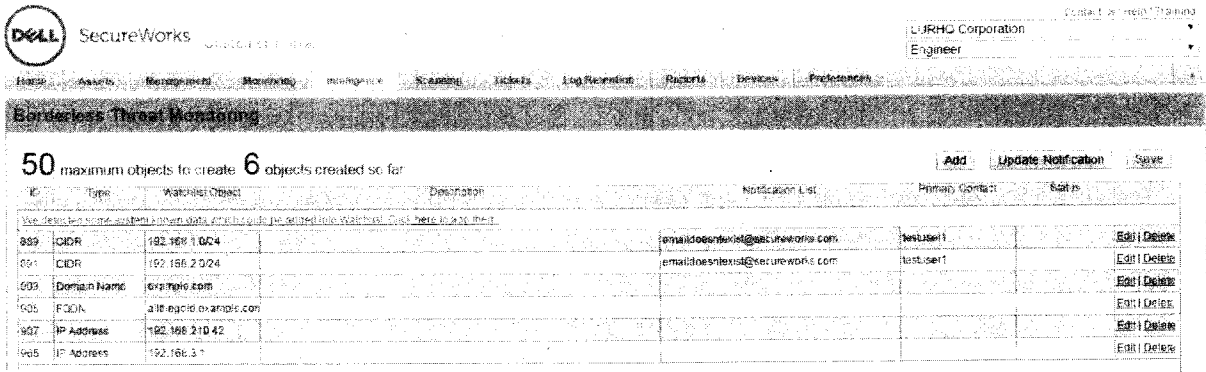
Schema Version:

Watchlists:

Revisions:

Borderless Threat Monitoring

The Borderless Threat Monitoring ("BTM") Service proactively provides contextual, actionable network threat indicator alerts that are specific to Customer which aids Customer in the decision-making processes as it relates to Customer's development of its' defensive measures and response processes and procedures. Borderless Threat Monitoring subscribers use the Portal to provide a Threat Profile consisting of Customer-owned identifiers. CTU researchers will vet the list to ensure Customer ownership of identifier contents using such information as Domain and Internet Number registrar databases as well as other Open Source resources.



Borderless Threat Monitoring

50 maximum objects to create 6 objects created so far

[Add](#) [Update Notification](#) [Save](#)

ID	Type	Watchlist Object	Destination	Notification List	Primary Contact	Status
999	CIDR	192.168.1.0/24		emaildoesnotexist@secureworks.com	testuser1	Edit Delete
991	CIDR	192.168.2.0/24		emaildoesnotexist@secureworks.com	testuser1	Edit Delete
993	Domain Name	example.com				Edit Delete
995	FQDN	all-ajcidr.example.com				Edit Delete
997	IP Address	192.168.2.10.42				Edit Delete
995	IP Address	192.168.3.1				Edit Delete

Customer Input

The Customer Threat profile is comprised of network identifiers owned by the Customer, such as:

- Mission critical IP addresses
- Domain names
- IP address ranges (e.g., CIDR blocks)
- Quantity of Threat profile identifiers will be determined by identifiers purchased by Customer (e.g. 10, 25, 50, 100).

Proactive Monitoring For Related Threat Indicators

Dell SecureWorks will proactively monitor multiple intelligence sources for network threat indicators related to the Customer Threat profile, to include:

- Network indicators from malware collected and processed by Dell SecureWorks
- Network indicators from Dell SecureWorks Threat research for known attack infrastructure and associated tradecraft
- Network indicators from botnets monitored by the CTU research team

Customer will receive event alerts via Portal tickets when Threat data is found related to Customer's Threat profile. Event alerts will contain the Customer Threat profile identifier, contextual indicators, and information about the identified Threat.

Delivery Options

Portal Access

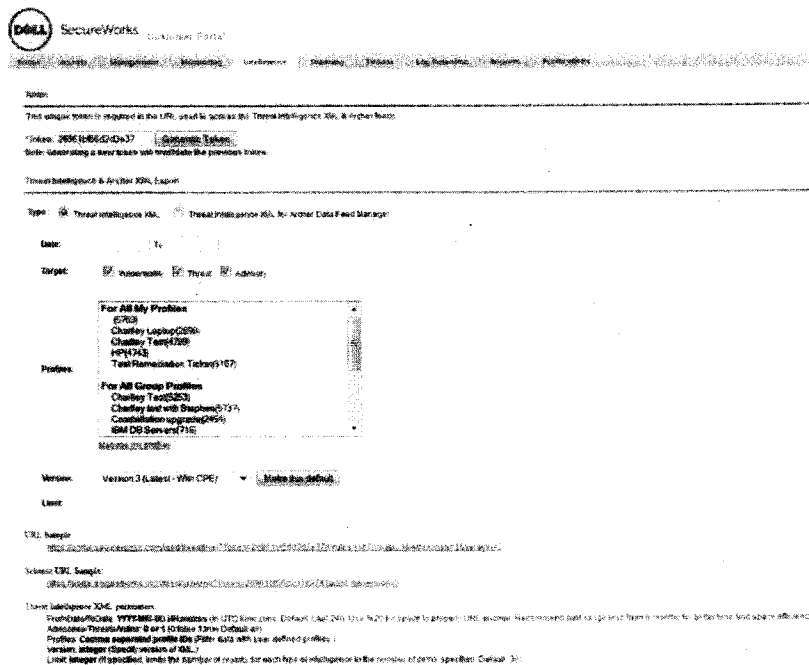
All TI Service customers will have access to the Portal. The Portal provides reports, search criteria, and a help desk ticketing system.

- The Portal provides on demand access to all Advisories, Threats, and Vulnerabilities via searchable reports.
- Applications can be mapped to assets and assigned a criticality to drive risk reporting and customize CTU TI data.
- The Portal provides a help desk ticketing system that can be used to escalate issues to Dell SecureWorks' security operations center ("SOC").

XML Data Feed Service Description/Deliverables

An XML data feed of Threats, Vulnerabilities, and Advisories is available in the Portal. The XML feed allows TI Service customers to export CTU TI data systematically into the Customer's own ticketing systems. The XML Data feed option is only available with the Enterprise TI Service Purchases.

- All Advisory, Threat, and Vulnerability data is available in XML format from the Portal.
- Typically, a Customer utilizing the XML feed will configure their ticketing system to pull CTU TI data every few hours.



The screenshot shows the Dell SecureWorks Customer Portal interface. The top navigation bar includes links for Home, About Us, Support, My Account, My Alerts, My Reports, My Settings, My Tickets, My History, My Profile, and My Logout. The main content area is titled "Threat Intelligence & Advisory XML Export". It contains a form for configuring the XML feed. The "Type" section has two radio buttons: "Threat Intelligence XML" (selected) and "Threat Intelligence XML for Another Data Feed Manager". The "Date" section has a dropdown menu set to "1". The "Target" section has three radio buttons: "Internal" (selected), "Physical", and "Advisory". The "Profiles" section has two expandable lists: "For All My Profiles" and "For All Group Profiles". The "Version" section has a dropdown menu set to "Version 3 (Latest - Win CPE)" and a "Make this default" button. The "Limit" section has a text input field. Below the form, there is a "URL Sample" section showing a sample URL for the XML feed. At the bottom, there is a "Threat Intelligence XML Description" section providing details about the feed's format and usage.

Service Level Agreements (SLAs)

The following SLAs shall apply to the TI Services provided hereunder, subject to the terms, conditions and limitations contained herein:

Service	Service Level Commitment	SKU
Vulnerability Data	<p>Vulnerabilities have a maximum time for publication based on each Vulnerability's severity. Time for publication is defined as the time from when a Vulnerability is disclosed to when it is published in the Portal.</p> <p>90% of Vulnerabilities will be published within three (3) business days of public disclosure.</p> <ul style="list-style-type: none"> Typically Vulnerabilities will be published within one (1) business day. SLA is measured on an annual percentage rate. 	
Threat Data	A minimum of two (2) Threat analyses will be provided per month.	
Microsoft Update Summary	A Microsoft Update Summary report will be provided within one (1) business day of a critical Microsoft operating system patch being releases by Microsoft?	
Microsoft Update Analysis	A Microsoft Update Analysis report will be provided within one (1) business day of a critical Microsoft operating system patch being released by Microsoft?	
Monthly Security Intelligence Webinar	At least one (1) security intelligence webinar will be delivered per month.	
Threat Intelligence Support	<p>Customers can initiate TI Support Service requests, to include telephone call-back requests by opening a ticket in the Portal. Tickets can be opened directly in the Portal web interface, by email message, or by a telephone call to the Dell SecureWorks SOC from an authorized user of an active TI Service with an active Customer Portal account.</p> <p>For Malware analysis requests, Customer will provide sample file(s) for analysis via the Portal ticket in password-protected .ZIP file along with related context / questions. A CTU researcher will provide initial assessment within one (1) business day of receipt of the ticket in response to the ticket. Customer may request additional analysis based on initial assessment within limits of the active TI Support Service. The CTU research team will negotiate further delivery with Customer based on</p>	TI-ADDON-Support



	<p>complexity of analysis.</p> <p>CTU will research TI Support Service requests and response via Portal ticket within one (1) business day of ticket creation. Service requests will be worked sequentially in the order received unless otherwise stack-rank prioritized by Customer. TI Support requests submitted outside of the Portal ticketing system will be addressed on a best-effort basis and are outside the scope of SLA.</p> <p>Requests for telephone call-back should contain Customer's point of contact name, telephone number, and nature of the research topic or issue. CTU research will respond via telephone call-back within one (1) business day to the Customer contact provided.</p> <p>TI Support Service utilization is capped at up to five (5) hours of CTU research time per month per unit of TI Support Service purchased. Unused TI Support Service capacity not utilized does not carry over from one month to the next.</p> <p>Customer may request a summary of TI Support Service utilization at any time by submitting a ticket request. CTU research will respond with the number of TI Support Service requests and number of total hours of TI Support Service used for the requested time period.</p> <p>CTU research reserves the right to decline TI Support Service requests which are beyond the scope of TI Support Service as defined in this service description, beyond the capability to deliver within contracted service levels, or may violate legal or regulatory requirements.</p> <p>TI Support Service requests are transactional. Requests for new recurring deliverables are beyond the scope of the TI Support Service.</p>	
AttackerDB Data Feed	AttackerDB data is accessible through the Dell SecureWorks Portal in both CSV and XML format.	TI-ADDON-ADB
Borderless Threat Monitoring	The CTU research team will process Customer Threat profile input (number of items determined by service level) for inclusion into Customer Threat profile within one (1) business day of submission by Customer. Threat profile input will be vetted by CTU researchers to ensure ownership by Customer. The CTU research team reserves the right to question and/or refuse requested updates to the Customer Threat profile if ownership of Customer-provided identifiers results in information outside of Customer-specific quality Threat indicators (e.g.	TI-ADDON-BTM-#



	Customer competitors and unlawful input). Customer will receive a BTM ticket via the Portal as new Customer Threat indicators are identified.	
Emerging Threat Bulletins	Bulletins are provided during normal business hours. A minimum of five bulletins will be provided each week.	
Weekly Intelligence Summary	One summary to be provided weekly.	
Bi-Weekly Cyber Security Roundup	Two (2) Cyber Security Roundup reports published per month.	

In the event that an SLA outlined above is not met, the Customer shall be entitled to receive an SLA credit (subject to procedures outlined in the Additional Service Rules, Regulations, and Conditions section below) equal to 1/30th of the monthly Service fee for the applicable Service affected, for each business day that the SLA is not met.

Additional Terms and Conditions

- a. Initiation of Dell SecureWorks' TI Service does not achieve the impossible goal of risk elimination and, therefore, Dell SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on the Customer's network.
- b. Dell SecureWorks may schedule maintenance outages with 48-hours' notice to designated Customer contacts.
- c. The Customer will receive credit for any failure to meet an SLA outlined above within thirty (30) days of Customer's notification to Dell SecureWorks of such failure. In order for the Customer to receive an SLA credit, the notification of the SLA failure must be submitted to Dell SecureWorks within thirty (30) days of the failure. Dell SecureWorks will research the request and respond to the Customer within thirty (30) days from the date of the request. The total amount credited to Customer in any calendar month in connection with any SLA outlined above will not exceed the Service fees paid by the Customer for such month. Except as otherwise expressly provided, the foregoing shall be the Customer's exclusive remedy for failure to meet or exceed the foregoing SLA.

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 4: Managed Web Application Firewall Service Description and Service Level Agreements



Managed Web Application Firewall Service Description and Service Level Agreements

This Service Description and Service Level Agreement (the "Service Description") describes the Service (as defined below) being provided to you ("Customer" or "you") by the Dell entity identified in the service order ("Service Order") executed by Customer and such Dell entity for the purchase of this Service. The Dell entity identified in the Service Order hereafter shall be collectively referred to as "Dell SecureWorks". This Service is provided in connection with Customer's signed Service Order and separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security and consulting services. In the absence of either a master services agreement or security services schedule, the Services performed under this Service Description are governed by and subject to the terms and conditions of the Dell SecureWorks Master Services Agreement, available at <http://Dell.com/Securityterms> which is incorporated by reference in its entirety herein (the "MSA").

Service Overview

The Dell SecureWorks Managed Web Application Firewall Service ("Service") consists of management and monitoring of one or more web application firewall device(s) ("Device(s)").

Management activities include Device provisioning, deployment, tuning and policy-based changes (including on a per-application basis as needed), as well as vendor software and firmware updates. Monitoring activities include collection, storage, reporting, and Customer notification of security events or Device health events. Tools for self-service reporting and analysis are provided through the CTP Customer portal ("Portal").

Service Features

Dell SecureWorks will deploy, manage, and monitor Customer's web application firewall Devices. Deployment will consist of project management, solution design, and provisioning. Management will consist of establishing a baseline policy, tuning rules, executing change requests, reviewing signatures, and updating software. Monitoring will consist of health and security event analysis and response. Reports and ticketing will be available through the Portal.

Standard Device Provisioning

Device Provisioning refers to the service setup activities for the managed Devices. The Device Provisioning period begins at receipt of the signed Service Order ("SO") by the MSS Deployment Team and ends with the scheduling of the Service Activation/Installation call with Customer.

The provisioning and setup period is dependent on a number of factors, such as the number of Devices, the number of applications, the number of physical sites, the complexity of the network and Customer requirements, and the ability of Customer to provide Dell SecureWorks with requested information within a mutually agreed-upon timeframe. Dell SecureWorks does not provide SLAs for completing Device service setup within a specified period of time.

Device Provisioning activities include:

- Scheduling Kick-off call (Receipt of SO by MSS Deployment Team is required)
- Information Gathering (Key requirements are a completed WAF Questionnaire and a network diagram.)



- Creating (on an as needed basis determined by Dell SecureWorks) a solution architecture diagram (Dell SecureWorks receipt from Customer of complete and accurate information and diagrams is required.)
- Configuring Customer Relation Management ("CRM") / Ticket system (Customer approval of MSS solution design diagram(s) is required.)
- Configuring the Device (Customer approval of solution design diagram(s), if applicable, is required.)
- Shipping the Device via ground shipping (Completion of Device configurations is required.)
- Scheduling of Service Activation call with Customer (Dell SecureWorks receipt of Customer acknowledging equipment is properly racked and cabled (with Out of Band if appropriate)) is required. Dell SecureWorks will begin tuning, monitoring and responding on a per-application basis on an agreed-upon schedule.

The following Device, location, and time-frame assumptions are used for purposes of providing a standard project-based timeframe for a Provisioning project plan:

- 1-4 Devices total, up to 4 applications total
- 1 physical location
- Dependencies external to Dell SecureWorks such as Customer-provided information and shipping carrier responsibilities are not included within the provisioning estimate.

Based on these assumptions, Dell SecureWorks can generally provision the Device(s) within five (5) weeks, not including the time required for Customer activities. As noted above, individual application monitoring and response will be activated on an agreed schedule.

CTP Customer Portal

Dell SecureWorks provides Customer with access to the secure Portal. The Portal may only be accessed by those named individuals specified by Customer during the Information Gathering phase and identified on the Service Initiation Form ("SIF") or by those who have been added to the list of named individuals after Service Activation. All information received by Customer through the Portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization without written authorization from Dell SecureWorks.

24x7 SOC Access

Customer may contact the Dell SecureWorks Security Operations Center ("SOC") 24 hours a day, 7 days a week, and 365 days a year via the Portal or telephone.

- The SOC can provide assistance with troubleshooting possible Device-related incidents.
- The SOC can change contact information or reschedule change times.
- The SOC cannot provide general consulting advice that does not directly pertain to the results of the Service.

(Optional) High Availability ("HA")

As an optional Service upgrade, Dell SecureWorks offers a High Availability solution for web application firewalls that natively support High Availability. This solution involves a firewall pair deployed in an active/standby or active/active configuration. In the event that the primary firewall fails, the secondary firewall is automatically engaged based upon the vendor technology for continuous service. When selected, this feature will be billed monthly, and billing for the HA pair will commence when the secondary Device is turned up. The first month will be billed in arrears; thereafter, HA will be billed monthly in advance.



Counter Threat Appliance ("CTA")

The CTA is a Dell SecureWorks-proprietary appliance that may be used in the secure delivery of the Service for either Device management or health/security event acquisition and transport. Dell SecureWorks may require that one or more CTAs be deployed in Customer's environment. For Services requiring the use of the CTA, Customer is responsible for ensuring that the implementation site complies with Dell SecureWorks' physical/environmental requirements.

Initial Implementation Support

Initial Implementation consists of the activation of a Device. During Initial Implementation, Dell SecureWorks will provide remote telephone support to validate that the Device is performing in Customer's network as designed (*e.g.*, Customer traffic is passed or rejected appropriately, interface connectivity has been established) and confirming our management capabilities (Dell SecureWorks has connectivity to the Device over the public network and is receiving expected data from the Device). Such telephone support will be provided during Eastern US time zone business hours.

(Optional) 24x7 Initial Implementation Support

Initial Implementation Support is provided as described above, but with a 24 hour a day, 7 day a week, and 365 day a year scheduling window and support, except Dell SecureWorks Business Holidays. Scheduling in advance is required for this Support. The Dell SecureWorks Business Holiday schedule can be provided upon written request. When selected, the Non-recurring Charge for this feature will be billed upon delivery.

(Optional) Re-provisioning Support

Re-provisioning Support is an orderable option for the Service. Re-provisioning Support may be ordered subject to a separate signed Statement of Work.

If Customer changes the Device's physical location or IP space or makes other significant modifications that impact Dell SecureWorks' delivery of the service, the Device will be subject to a re-provisioning fee. Examples include:

- Change External IP of Device
- Device Physical Move (without change of IP address or objects)
- Device Physical Move (with change of IP address and objects)
- Participate in Failover Testing or Perform Route Swapping between multiple Devices
- IP Re-numbering of interface(s) and associated objects
- Swapping to new supported hardware of a different make or vendor
- Re-organizing policy based on groups or other standard
- Consolidating multiple Device policies (priced per Device)
- Major revision of a protected application, Certificate implementation or updates on Device

(Optional) Out of Band ("OOB") Hardware (CTA)

For purposes of Device maintenance and troubleshooting, Dell SecureWorks will provide an optionally-orderable element of the Service – equipment that will enable the SOC to remotely and securely connect to the Dell SecureWorks CTA. Additional charges may apply.

For each CTA at Customer's site, Customer shall make permanently available one analog telephone line ("POTS line") or additional IP address for each CTA. Dell SecureWorks will provide equipment to be attached to this line to provide OOB access. Upon mutual agreement by the parties, Customer's

existing OOB access option may be used where appropriate. Service interruptions or failure to achieve the SLAs will not be subject to penalty in the event of noncompliance with the above.

(Optional) Out of Band ("OOB") Hardware (Device)

For purposes of Device maintenance and troubleshooting, Dell SecureWorks can provide an optionally-orderable element of the Service – equipment that will enable the SOC to remotely and securely connect to the Device. (e.g., web application firewall)

Dell SecureWorks can provide equipment to be attached to the POTS line and/or additional IP address in order to provide OOB access for Customers who choose this option. Upon mutual agreement by the parties, Customer's existing OOB access option may be used where appropriate. Service interruptions or failure to achieve the SLAs will not be subject to SLA Credit in the event of noncompliance with the above.

Return Merchandise Authorization ("RMA") Process Responsibilities

Customer is responsible for initiating and fulfilling the RMA process with their 3rd party vendor in the event that the Hardware/Software being managed by Dell SecureWorks is determined to be in a failed or faulty state that requires replacement.

Software Upgrade and Patch Maintenance

Dell SecureWorks monitors all vendors represented on Dell SecureWorks' approved platforms list for release activities related to software patches and upgrades. As security related software patches and upgrades are released, Dell SecureWorks assesses the applicability of each release to Customer's environment. Dell SecureWorks will work with Customer to schedule any necessary remote upgrades.

Patches are applied at no additional charge. Customer-Owned Equipment upgrades are implemented by Dell SecureWorks as part of the selected service, so long as the following conditions apply:

- The upgrade can be performed remotely, either independently or with a minimal amount of on-site assistance by Customer.
- The upgrade does not require a change to underlying hardware on which Customer-Owned Equipment is deployed.
- A single upgrade does not require more than 2 person-hours of Dell SecureWorks' time. If additional time is required, it will be performed on a time and materials basis pursuant to a separate Statement of Work.

Dell SecureWorks will bill Customer for all work beyond the allocated 2 hours and for any work that requires a Dell SecureWorks employee to travel to Customer's site. If the upgrade requires any additional licensing or maintenance fees, Customer will be responsible for these fees.

In cases where support for a particular product or product version is being discontinued by the vendor or by Dell SecureWorks, Dell SecureWorks will communicate new platform migration options. To be assured of uninterrupted service, Customer must complete the migration process within 60 days. Customer bears any costs relating to procuring new hardware or components and to re-provisioning any devices.

SLAs do not apply during maintenance work. In addition, SLAs cannot be guaranteed if Customer does not make the changes required by Dell SecureWorks or if Customer prevents Dell SecureWorks from making the changes it notifies Customer are necessary for continued service.

Defective Hardware Replacement

As part of the Service, Dell SecureWorks will perform remote Hardware replacement for Devices declared by the vendor as defective. Customer-provided replacement hardware must be the same vendor make and model as the defective Device.

Hardware Upgrades

At our discretion, Dell SecureWorks may agree to perform same-vendor Hardware upgrades for Customer. Upgrades due to Customer's wish to upgrade the vendor model or product EOL, etc. will incur additional fees.

Web Application Scan Policy

Dell SecureWorks will incorporate Web Application Scan results into the WAF policy on a per application basis, up to one time per week (seven calendar days). Web Application Scan results identify application vulnerabilities and exposures. This information will be used by the Dell SecureWorks SOC to enhance the WAF policy in order to detect and prevent threats that may compromise exposures identified by the Web Application Scan technology. Since applications change over time, we will incorporate Web Application Scan results on a recurring basis.

Customer is required to subscribe to Dell SecureWorks' Web Application Testing Service delivered by Dell SecureWorks Security and Risk Consulting, the Web Application Scanning Service delivered by Managed Security Services, or provide its own Web Application Scan results to benefit from the Web Application Scan integration with the Service. The application scan engine must be supported by the managed WAF technology.

Critical Event Processing Acceptance of Ticket

A Critical Event is any event that, in Dell SecureWorks' judgment, warrants notification to Customer as specified in a Service Level Agreement. All security events are categorized based on severity level. When a Critical Event is detected by our event processing platform, a ticket is automatically generated and qualified by the SOC. **NOTE:** The Dell SecureWorks SOC does not monitor and respond to simulation-mode events, only to active mode events. This transition occurs at the end of the initial tuning process.

Critical Event Processing Customer Notification

All security events are categorized based on severity level. When a Critical Event is detected by our event processing platform, a ticket is automatically generated and qualified by the SOC. Dell SecureWorks then contacts Customer within the time specified in the relevant SLA and in the manner specified by Customer during Provisioning.

Device Unreachable Monitoring Acceptance of Ticket

Upon determination that a Device is unreachable via the public network, the Dell SecureWorks platform creates an incident ticket. This is based upon the time between the creation of the ticket by the platform and the time the SOC formally begins to process the ticket. The SOC will begin to act on the ticket in accordance with the SLA.

Device Unreachable Monitoring Outbound Notification

Upon acceptance of an incident ticket, the SOC performs an analysis to qualify the validity of the reported event. This SLA refers to the time between the SOC's formal acceptance of the ticket and initiation of Customer notification process. The SOC will begin the notification process in accordance with the SLA.

Event Flow Disruption Check

Upon determination that Dell SecureWorks has stopped receiving events from a Device, the Dell SecureWorks platform creates an incident ticket. The SOC performs analysis to qualify the validity of the reported event and then initiates Customer Notification process.

Health and Performance

Upon determination that a Device has met pre-defined health or performance thresholds of concern via checks conducted over the public network, the Dell SecureWorks platform creates an incident ticket. Upon acceptance of an incident ticket, the SOC performs an analysis to qualify the validity of the reported event and then initiates Customer notification process.

Signature Updates

Dell SecureWorks will update WAF signatures on a recurring basis following release from vendor. The updates are deployed in the following manner:

- Automatically deployed updates from the vendor
- On-demand updates from the vendor per Customer request
- At Customer request, Dell SecureWorks will not deploy vendor updates

Security Event Reporting

All security events are available for viewing and reporting on the portal. The portal provides a secure mechanism to create, customize, and access "executive" and more technical level reports, as well as view and report on detailed and historical event data. The portal enables Customer to create both standard and customized reports that can be named, scheduled to run at regular or one-off intervals, automatically emailed, or forwarded for review and sign-off for audit/sign-off purposes.

Service Activation

Service Activation consists of three main phases: Information Gathering, CTA Deployment (when appropriate), and Service Provisioning and Installation.

Information Gathering

When Dell SecureWorks receives the Services Order, Dell SecureWorks provides Customer with a Service Initiation Form ("SIF") to be completed by Customer. When Customer returns the completed Service Activation Profile ("SAP"), Dell SecureWorks schedules a conference call to review the completed document and other relevant information.

CTA Deployment

Using data gathered during the Information Gathering phase, Dell SecureWorks determines the number of CTAs required and the appropriate deployment location(s) within Customer's environment.

If changes to Customer's existing network architecture are required for Service implementation, Dell SecureWorks communicates these changes to Customer.

Dell SecureWorks reserves the right, in its reasonable discretion, to utilize one or more CTAs deployed in a Dell SecureWorks data center ("hosted CTA") to communicate with Devices that Dell SecureWorks is managing and monitoring, in lieu of deploying CTA(s) for use in Customer's network. In such case, the terms and conditions pertaining to the CTA do not apply.

Service Provisioning and Installation

The Service Provisioning and Installation phase begins upon the completion of the Information Gathering phase. Service Provisioning and Installation is performed in the following manner:

1. New Devices to be deployed are shipped directly to Dell SecureWorks for configuration and subsequent shipment to Customer location.
2. Existing equipment in use is provisioned remotely, when possible, with on-site support from Customer. If on-site support from Dell SecureWorks is required, a consulting engagement must be executed under a separate SOW.
3. Dell SecureWorks provides telephone support to Customer contact at the implementation site during installation of all Customer premises equipment.
4. Once Customer premise equipment is in place, Dell SecureWorks accesses the Device(s) remotely and performs the remaining configuration and Service activation tasks which may require Device downtime.

IMPORTANT: Customers must provide Dell SecureWorks with administrative/root privileges on the specific Devices to be managed.

Service Commencement

Dell SecureWorks will provide Customer with a Notice of Service Commencement, which identifies the Service Commencement Date, when Dell SecureWorks has:

- a. Established communication with the relevant Customer device(s) and CTA(s)
- b. Verified availability of Customer data on the portal
- c. Established communications via OOB (where available)

Ongoing Monitoring and Management

This section provides an overview description of Dell SecureWorks' 24x7 WAF management and monitoring activities.

Policy Management

Dell SecureWorks manages the policy on the Device. The policy will be tuned so that each signature is classified by an action (block, monitor only, or no alert) and by a severity level. Critical events are events that Dell SecureWorks views as significant risks to Customers. These events may require immediate notification and swift resolution by Dell SecureWorks or Customer. Dell SecureWorks determines which events belong at the Critical Severity level through the use of signature priorities, event correlation, and professional judgment. All other event severity levels are events that Dell SecureWorks does not believe pose an immediate threat or risk.

When tuned to active mode, all traffic matching the signature will be blocked. Customer will be able to view blocked traffic on the portal. When tuned to simulation mode, traffic matching the signature will not block traffic. However, Customer can view and assess this traffic on the portal to determine if and when it is appropriate to enable blocking.

Dell SecureWorks is not responsible for negative impacts to Customer as a result of network traffic blocked by the Device. Dell SecureWorks will work with Customer to tune the policy during the initial tuning period.

Customers may request that a signature or alert be blocked, unblocked, or reprioritized by calling Dell SecureWorks or opening a ticket via the portal. This activity is not subject to a SLA.

Initial Policy Tuning

Upon service activation, Dell SecureWorks applies one baseline policy to each Device. Dell SecureWorks then tunes the policy to Customer's environment during a period that is approximately forty five (45) calendar days, which begins on the Service Commencement Date. During this tuning period, Dell SecureWorks works with Customer to determine the action and severity applied to signatures, based on WAF device learning as it receives traffic, as well as Dell SecureWorks' familiarity with Customer's applications and optimal configuration. This period may vary depending on the complexity of the deployment, number of applications, and other factors, and is not subject to a SLA.

Policy and Configuration Maintenance

Policies are updated regularly as updates are released by vendors and reviewed by Dell SecureWorks for efficacy and proper operation.

If supported by the Device, Dell SecureWorks can configure the Device to fail open or closed, depending on Customer preference. In the event of Device failure, if the Device configured to fail open, no traffic will be blocked; if configured to fail closed, all traffic will be blocked.

Device Uptime Monitoring

Dell SecureWorks performs two kinds of monitoring services:

- Device Uptime Monitoring
- Security Event Monitoring

Dell SecureWorks will check for indicators that Devices are up and running or "healthy." Health indicators refer to Device uptime checks, system resource checks, and critical process checks.

Supportable health checks may differ according to vendor products, service delivery architectures, and Customer policy. In addition, Dell SecureWorks will periodically poll the Dell SecureWorks database for events received from each Device. If a failed or negative response is received from any of the checks, an automatic alert is sent to Dell SecureWorks.

Dell SecureWorks will attempt to qualify alerts before notifying Customer. After Customer notification, Dell SecureWorks may perform further troubleshooting or remediation steps after the root problem is identified.

If...	Then...
The underlying issue lies with the Device managed by Dell SecureWorks,	Dell SecureWorks will attempt to resolve the problem by working with Customer's designated point of contact via phone to address any Device related problems.
The underlying issue is Customer related, such as network change, outage, or Customer-managed Device,	Dell SecureWorks will provide Customer with available troubleshooting information, but Dell SecureWorks is not responsible for troubleshooting issues that do not directly relate to the Device, CTA, or Dell SecureWorks' network.

Security Event Monitoring

Security event data is sent to a Customer-premise-based CTA or hosted CTA depending on how the Service is architected. In either case, the data is parsed, normalized, correlated, and prioritized. All security events are categorized by Dell SecureWorks based on severity level.

When a Critical Event is detected, initial correlation, de-duplication, and false positive reduction is performed by the correlation engine. If the event is confirmed as a Critical Event, a ticket is automatically generated. Dell SecureWorks then contacts Customer within the time specified in the relevant SLA. Dell SecureWorks also performs additional analysis to determine whether the event is a false positive.

Dell SecureWorks provides Customer with a description of the event and any contextual information. The event is also posted on the portal and made available for reporting. However, in-depth analysis, incident response, forensics, and countermeasures (other than policy changes to the Device or other Dell SecureWorks managed Device) are not included in this service. Dell SecureWorks can provide these areas of advanced support as a consulting engagement under a separate, signed Statement of Work.

Device Management

Device Management Service activities consist of:

- Software Updates and Patches
- Software Upgrades
- Hardware Upgrades
- Hardware Replacement

Dell SecureWorks monitors all vendors represented on Dell SecureWorks' approved platforms list for release activities related to software patches and upgrades. As security related software patches and updates are released, Dell SecureWorks assesses the applicability of each release to Customer's environment. Dell SecureWorks will work with Customer to schedule any necessary remote updates.

SLAs do not apply during maintenance work. SLAs cannot be guaranteed if Customer does not make the changes required by Dell SecureWorks or if Customer prevents Dell SecureWorks from making the changes it notifies Customer are necessary for continued service.

Equipment

Customer Owned Equipment

Customer is responsible for maintaining valid maintenance agreements for all Customer-Owned Equipment to be deployed in conjunction with the Service.

To the extent Dell SecureWorks is performing Services using Customer-Owned Equipment, Customer agrees to:

- a. Provide Dell SecureWorks with reasonable and safe access to Customer-Owned Equipment necessary for Dell SecureWorks to perform the Services, including licenses and all associated information that is required to activate and operate the Device, which may include feature or activation codes, platform serial number or IP address.
- b. Secure any licenses, approvals, or consents required for Dell SecureWorks to access or use Customer-Owned Equipment necessary for Dell SecureWorks to perform the Services.
- c. Procure all vendor maintenance agreements required for Dell SecureWorks to provide the Services.

Customer agrees not to alter, modify, or re-configure Customer-Owned Equipment without reasonable advance notification to Dell SecureWorks. If Customer-Owned Equipment fails in the field, Customer is responsible for providing a replacement. The replacement must be shipped directly to Dell SecureWorks for configuration and subsequent shipment to Customer location. Once a Customer has a replacement on-site, Dell SecureWorks will provide reasonable telephonic support to Customer.

to restore the Service. SLAs do not apply until Customer has replaced the failed equipment and Dell SecureWorks has established that it can communicate with and monitor events from the new Device.

In cases where support for a Device is being discontinued by the vendor or Dell SecureWorks, Dell SecureWorks will communicate new platform migration options. In order to be assured of uninterrupted service, Customer must complete the migration process within the timeframe in the Dell SecureWorks End of Life ("EOL") announcement. Customer bears any costs relating to procuring new hardware or components or to the re-provisioning of any Devices.

SLAs do not apply during maintenance work. Service continuity cannot be guaranteed if Customer does not make the changes required by Dell SecureWorks.

Dell SecureWorks Equipment

If Dell SecureWorks Equipment becomes unavailable or unreachable, Dell SecureWorks will troubleshoot the issue. If Dell SecureWorks concludes that the Dell SecureWorks Equipment has failed and is not restorable, Dell SecureWorks will ship a replacement unit.

SLAs do not apply during the period during which Service is unavailable. Replacement Device(s) will be re-provisioned according to the Provisioning process.

Virtual Environments

Dell SecureWorks offers management for the Imperva® SecureSphere Virtual Appliance family and F5 Networks BIG-IP® Application Security Manager™ (ASM) VE virtual appliances, both on VMware ESX/ESXi in Network mode. Customer is responsible for all aspects of installation, configuration, and setup of VMware, including but not limited to:

- Virtual Switches (vSwitch)
- Virtual Network Interfaces (vNIC)
- Virtual Networks
- Virtual Machines (VM)

Customer is responsible for providing the Virtual Machine(s) with the minimum CPU, memory, and network resources needed for proper functionality as specified by the web application firewall vendor.

Customer shall provide Dell SecureWorks with a privileged account on the appliance and a privileged vSphere account with access to the Virtual Machine(s). In a fully managed scenario, Dell SecureWorks shall maintain exclusive administrative privilege to the virtual appliance. Upon Customer request, read-only access to the virtual appliance may be provided to Customer. Customers who have read-only access to the virtual appliance will be notified in advance of any work being done on the virtual appliance.

For Out Of Band (OOB) access and maintenance scenario situations, the "vSphere account" should have privileges to perform the following actions:

- Power off
- Power on
- Power reset
- Console

Customer Obligations and Interdependencies for Dell SecureWorks Performance

Customer agrees to perform the following obligations and acknowledges and agrees that Dell SecureWorks' ability to perform its obligations and its liability under the SLAs below depend on Customer's compliance with the following:

- Customer is responsible for purchasing the web application firewall hardware and software necessary for the managed web application firewall service.
- Customer is responsible for providing access to Customer premises and relevant appliance(s) and management console(s).
- Customer is responsible for maintaining appropriate levels of software and hardware support and maintenance (including third party hardware and software contracts and licenses) and connectivity to prevent network performance degradation and maintain communications between Customers contracted devices and Dell SecureWorks platform.
- Customer is responsible for making available to Dell SecureWorks personnel with expertise related to the specific web application(s) being protected by the Service and providing assistance to Dell SecureWorks in developing an appropriate rule set in order to provide protection for the web applications being protected by the service offering.
- Customer is responsible for reviewing and approving the final rule sets for the web applications being protected by the service offering.
- Customer is responsible for masking confidential information logged by the WAF including but not limited to passwords, credit card numbers, social security numbers, and other personal identifiable information. Dell SecureWorks also may add data masking objects to customer WAF policies.
- Customer is responsible for implementing and maintaining effective password policies for external and internal applications.

Service Level Agreements (SLAs)

Service Level Agreement Matrix

SLA	Description	SLA Credit
Standard Change Request	<p>Change Requests (as defined below) identified as "Standard" will receive the following service levels:</p> <ul style="list-style-type: none"> Acknowledgement of receiving the change within 1 business hour from the time stamp on the ticket created by Dell SecureWorks 	1/30 th of monthly fee for Service for the affected device
All Other Ticket Requests	<p>Standard requests (applies to all non-change and non-incident tickets) submitted via the Dell SecureWorks CTP Customer portal or via telephone will be subject to "acknowledgement" (either through the ticketing system, email, or telephone) of receiving the request within one (1) hour from the time stamp on the ticket created by Dell SecureWorks.</p> <p>An acknowledgement to ticket requests classified as "Urgent" on the ticket and verified by the SOC as "Urgent" will be sent (either through the ticketing system, email, or by telephone) within fifteen (15) minutes from the time stamp on the ticket created by Dell SecureWorks.</p>	1/30 th of monthly fee for Service
Security Monitoring	<p>Customer shall receive a response (according to the escalation procedures defined in the CTP Customer portal or in the manner pre-selected in writing by Customer, either through the ticketing system, email, or by telephone) to security incidents within fifteen (15) minutes of the determination by Dell SecureWorks that given malicious activity constitutes a security incident. This is measured by the difference between the time stamp on the incident ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.</p> <p>A "security incident" is defined as an incident ticket that comprises an event (log) or group of events (logs) that is deemed high severity by the SOC in accordance with Dell SecureWorks' Event Handling Process (see Exhibit A). The most up-to-date version can always be found in the Real-Time Events section of the CTP Customer portal.</p> <p>Automatically created incident tickets (via correlation technology) and event(s) or log(s) deemed low severity will not be escalated, but will be available for reporting through the CTP Customer portal.</p>	1/30 th of monthly fee for Service for the affected device
Active Health Monitoring	<p>Device Unreachable – Dell SecureWorks will provide a 30 minute response (via phone, ticket, or email) from identification of the device being unreachable. This is measured by the difference between the time stamp on the device unreachable ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.</p>	1/30 th of monthly fee for Service for the affected device



Additional Service Rules, Regulations and Conditions

- a. The Service provides robust device management, security analysis, and performance monitoring to Customer. However, deployment of Dell SecureWorks' managed services in a Customer network does not achieve the impossible goal of risk elimination, and therefore Dell SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on a Customer network.
- b. Dell SecureWorks may schedule maintenance outages for Dell SecureWorks-owned equipment/servers which are being utilized to perform the services with 24-hours' notice to designated Customer contacts.
- c. The Service Levels set forth herein are subject to the following terms, conditions, and limitations:
 - i. The Service Levels shall not apply during scheduled maintenance outages, and therefore are not eligible for any Service Level credit during these periods. In addition, Dell SecureWorks shall not be held liable for any service impact or Service Levels Agreements related to product configurations that are not supported by Dell SecureWorks within Customer's policy.
 - ii. The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Dell SecureWorks from providing the Service, delivering the Service Levels or managed service descriptions, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by Customer, its employees, agents, or third parties acting on behalf of Customer.
 - iii. Furthermore, the Service Levels shall not apply to the extent Customer does not fulfill and comply with the obligations and conditions set forth within this SLA. The obligations of Dell SecureWorks to comply with the Service Levels with respect to any incident response or ticket request are also dependent on Dell SecureWorks' ability to connect directly to Customer devices on Customer network through an authenticated server in the Dell SecureWorks Secure Operations Center.
- d. Dell SecureWorks will troubleshoot and, if necessary, replace any iDevices in accordance with Exhibit B, "Dell SecureWorks Maintenance Program Terms and Conditions."
- e. Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Dell SecureWorks of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Dell SecureWorks within thirty (30) days of such failure. Dell SecureWorks will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the Agreement, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.

Exhibit A – Dell SecureWorks' Event Handling Process

Event Handling Process

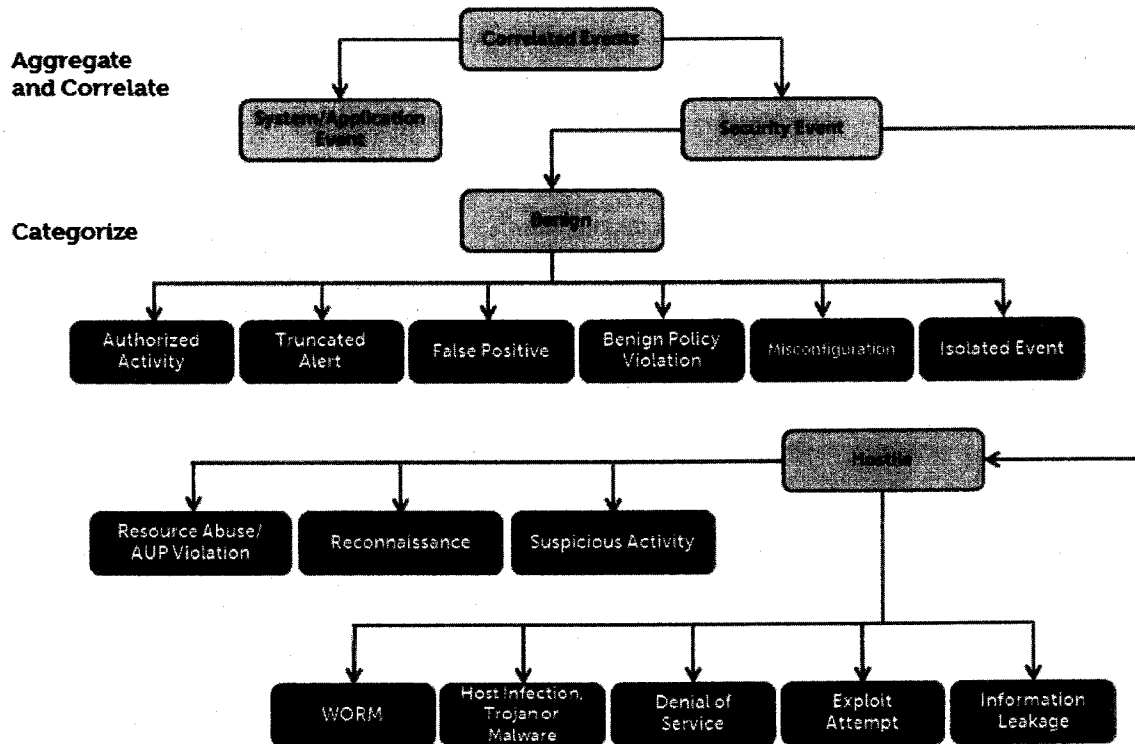


Exhibit B – Dell SecureWorks Maintenance Program Terms and Conditions

- Dell SecureWorks agrees, subject to the terms and conditions of your separate master service agreement or security services schedule (and as further set forth below), to replace Dell SecureWorks iDevices that are not properly functioning due to ordinary wear and tear, malfunctions, inadequate available memory, or obsolescence (the "Program"). Replacement devices may be new or refurbished.
- iDevices subject to this Program may include the Dell SecureWorks' Counter Threat Appliance (CTA), iSensor, LogVault appliance, Inspector, SDA, SYSLOG Aggregator, log collection devices, and/or SNORT IDS device.
- If Customer is purchasing an iDevice, the following terms apply:
 1. Mere purchase by Customer of an iDevice does not subject the same to this Program unless: (a) such iDevice is expressly specified in a written Dell SecureWorks Service Order or Service Agreement signed by an authorized officer of Dell SecureWorks and (b) Customer's payment of all maintenance fees is made when due.
 2. Customer may elect to participate in the Program only at the time of purchase of the Dell SecureWorks iDevice. If, at any time after the purchase of the Dell SecureWorks iDevice, Customer wishes to participate in this Program, it must agree to pay all fees that would have been billed since the actual date of purchase of the iDevice.
- The charges for the Program only cover replacement of Dell SecureWorks iDevices. Any performance, damage, repair and/or other warranty issues, or claims with respect to non-Dell SecureWorks-branded iDevices must be addressed with the applicable OEM manufacturer.
- Dell SecureWorks' obligation to comply with the foregoing is conditioned upon, and subject to, the assistance and availability of Customer's onsite personnel for assistance in the: (x) diagnosis and troubleshooting of problems with existing iDevices and (y) replacement and installation of any new iDevice all in compliance with your master service agreement or services schedule.
- Furthermore, Dell SecureWorks will not replace Dell SecureWorks iDevices returned by Customer that are no longer performing on account of unauthorized use, physical damage, or misuse or abuse of the products, as determined by Dell SecureWorks in its sole discretion, including, but not limited to, any of the following circumstances:
 1. Damage due to lightning or other climate problems (including, but not limited to, exposure to excessive light, heat, flooding, and the like)
 2. Opening of iDevices by any person other than Dell SecureWorks authorized personnel
 3. Unauthorized loading or modification of software on or other reprogramming of the iDevice
 4. Unauthorized linking of the iDevice with other Customer equipment or systems
 5. Cracks in iDevices, dents to chassis or apparatus, or other damage caused by dropping of iDevice or other mishandling, misuse, or abuse
 6. Presence of liquids (or residue there from) or the excessive presence of other extraneous materials inside the iDevice (including, but not limited to, dust, hair, dirt, or grime)
 7. Inability to mount the iDevice
 8. Improper powering down of the iDevice
- Dell SecureWorks shall bill Customer, and Customer shall be liable, for iDevices: (i) damaged due to misuse or abuse, or (ii) no longer performing adequately due to unauthorized use, physical damage, misuse, or abuse of the iDevices.



Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 5: Managed and Monitored Advanced Malware Protection Service Description and
Service Level Agreement



Managed and Monitored Advanced Malware Protection Service Description and Service Level Agreement

This Service Description and Service Level Agreement (SLA) is provided for the customer ("you" or "Customer") and the Dell entity identified in the Customer's Service Order ("SO") for the purchase of this Service (described below). This Service is provided in connection with the Customer's separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security services. In the absence of either a master services agreement or security services schedule, this service is provided in connection with the Dell SecureWorks Master Services Agreement, available at <http://Dell.com/Securityterms> and incorporated by reference in its entirety herein.

Service Overview

The Dell SecureWorks® Managed and Monitored Advanced Malware Protection ("AMP") Service ("the Service") provides proactive administration of your advanced malware protection infrastructure 24 hours a day, 7 days a week, and 365 days a year. Dell SecureWorks' certified security experts will perform all activities necessary to keep your devices operating at peak performance.

Managed and Monitored Advanced Malware Protection Service Tiers

This Service is offered according to various service tiers, including the Bronze, Silver, Gold and Platinum Service Level tiers. Depending on the level of service required, some features are optional. Stand-alone options may be purchased at an additional cost, either at the time of execution of the initial Services Order or later during the Service term, provided that Dell SecureWorks continues to make such options generally available for separate purchase.

- Bronze (Monitored AMP) – The Bronze Service Level tier provides real-time, security event analysis and response for any Advanced Malware events 24 hours a day, 7 days a week, 365 days a year. Dell SecureWorks Security Monitoring service combines our advanced Counter Threat Platform with a team of security analysts to deliver strong security and compliance value to our customers. This Service includes the following components described in detail below:
 - Managed Device Provisioning
 - Advanced Malware Protection
 - Counter Threat Platform Customer Portal
 - 24 x 7 SOC Access
- Silver (Monitored and Managed AMP) – The Silver Service Level tier includes the real-time, security event analysis and response for Advanced Malware events as described in the Bronze Service level, and additionally includes the following components described in detail below:
 - Managed Device Uptime Monitoring
 - Upgrade and Patch Management
 - Implementation of Replacement Hardware and Hardware Upgrades

- Management Console
- Change Management
- Gold (Monitored and Managed AMP with Advanced Event Analysis and Threat Context) – The Gold Service Level tier includes real-time, security event analysis and response and full appliance Management as described in the Silver Service level, and additionally includes the following components described in detail below:
 - Advanced Event Analysis and Threat Context
- Platinum (Monitored and Managed AMP with Advanced Event Analysis and Threat Context, and Customer Directed Research) – The Platinum Service Level tier includes real-time, security event analysis, full appliance Management and Advanced event analysis and treat context as described in the Silver Service level, and additionally includes the following components described in detail below:
 - Customer Directed Research for AMP Events

Service Level Tiers Matrix

- ✓ Denotes the feature is included with no additional fee or monthly recurring revenue (MRR) required
- Denotes the feature is optional with an additional fee or MRR associated
- Denotes the feature is not available under the specified Service Level

Service Features	Bronze	Silver	Gold	Platinum
Managed Device Provisioning	✓	✓	✓	✓
24x7 Event Monitoring, analysis and notification	✓	✓	✓	✓
24x7 SOC Access	✓	✓	✓	✓
Event consolidation and reporting	✓	✓	✓	✓
24x7 appliance health and performance monitoring	–	✓	✓	✓
Configuration tuning, software updates, patch and change mgmt.	–	✓	✓	✓
Deep-dive threat and contextual analysis for security events of interest	–	–	✓	✓
Event correlation with Dell SecureWorks' threat data from multiple intelligence sources	–	–	✓	✓
Customer directed research for MAMP events	–	–	–	✓
Incident Repose and Forensics	○	○	○	○

Service Description

Dell SecureWorks' proprietary platform and processes provide the foundation for delivery of our managed security services. Dell SecureWorks-developed technology and security procedures facilitate device management, health monitoring, security event analysis, and Customer reporting. The following service components may be included with the Service, as indicated by the service tier:

- Managed Device Provisioning
- Advanced Malware Protection
- Counter Threat Platform Customer Portal
- 24 x 7 SOC Access
- Managed Device Uptime Monitoring
- Upgrade and Patch Management
- Implementation of Replacement Hardware and Hardware Upgrades
- Management Console
- Change Management
- Advanced Event Analysis and Threat Context
- Customer Directed Research for AMP Events
- Other (Out of Scope) Services

Managed Device Provisioning

Managed Device Provisioning refers to the Service setup activities for the on-premise devices used to deliver the Advanced Malware Protection capability of the Service, as well as any associated management consoles used to manage the protection devices (collectively, "Managed Devices"). The Managed Device Provisioning period begins at receipt of the signed Service Order by the Managed Security Services (MSS) Deployment Team and ends with the scheduling of the Service Activation/Installation call with Customer.

The provisioning and setup period is dependent on a number of factors, such as the number of Managed Devices, the number of physical sites, the complexity of the network and of Customer requirements, and the Customer's ability to provide Dell SecureWorks with requested information within a mutually agreed-upon timeframe. Dell SecureWorks does not provide SLAs for completing Managed Device service setup within a specified period of time.

Managed Device Provisioning activities include:

- Scheduling Kick-off call with receipt of Service Order by MSS Deployment Team.
- Configuring Customer Relation Management ("CRM") / Ticket system. **NOTE:** Customer approval of MSS solution design diagram(s) is required.
- Configuring the Managed Device(s).
- Scheduling of Service Activation call with Customer. **NOTE:** Dell SecureWorks receipt of Customer acknowledgement that equipment is properly racked and cabled with Out of Band, if appropriate, is required. Dell SecureWorks will begin tuning, monitoring and responding on a per-application basis on an agreed-upon schedule.

It is the Customer's responsibility to procure and take delivery of the Managed Devices.

Counter Threat Appliance ("CTA")

The CTA is a Dell SecureWorks-proprietary appliance that is used in the secure delivery of the Service for either Managed Device management or health/security event acquisition and transport. Dell SecureWorks requires that one or more CTAs be deployed in Customer's environment. Customer is responsible for ensuring that the implementation site complies with Dell SecureWorks' physical/environmental requirements.

Initial Implementation Support

Initial Implementation consists of the activation of a Managed Device. During Initial Implementation, Dell SecureWorks will provide remote telephone support to validate that the Managed Device is performing in the Customer's network as designed; for example, Customer traffic is being evaluated and handled appropriately and interface connectivity has been established. Dell SecureWorks will also confirm our management capabilities by ensuring connectivity to the Managed Device over the public network and by ensuring receipt of expected data from the Managed Device. **NOTE:** Telephone support will be provided during Eastern US time zone business hours.

(Optional) 24x7 Initial Implementation Support

Initial implementation support is provided as described above, but with a 24 hour a day, 7 days a week, and 365 days a year scheduling window and support, except Dell SecureWorks Business Holidays. Scheduling in advance is required for this Support. The Dell SecureWorks Business Holiday schedule can be provided upon written request. When selected, the non-recurring charge for this feature will be billed upon delivery.

(Optional) Re-provisioning Support

Re-provisioning support is an orderable option for the Service. Re-provisioning support may be ordered subject to a separate signed Service Order.

If Customer changes a Managed Device's physical location or Internet Protocol (IP) space or makes other significant modifications that impact Dell SecureWorks' delivery of the Service, the Managed Device will be subject to a re-provisioning fee. Examples include:

- Managed Device External IP change
- Managed Device Physical Move (without IP address change or objects)
- Managed Device Physical Move (with IP address change and objects)
- Participation in Failover Testing or performing Route Swapping between multiple Managed Devices
- Interface(s) and associated objects IP Re-numbering
- Policy reorganization based on groups or other standards

(Optional) Out of Band (OOB) Hardware (CTA)

For purposes of CTA maintenance and troubleshooting, Dell SecureWorks will provide an optionally-orderable element of the Service – equipment that will enable the SOC to remotely and securely connect to the Dell SecureWorks CTA. **NOTE:** Additional charges may apply.

For each CTA at Customer's site, Customer shall make permanently available one analog telephone line (POTS line) or additional IP address for each CTA. Dell SecureWorks will provide equipment to be attached to this line to provide OOB access. Upon mutual agreement by the parties, Customer's existing OOB access option may be used where appropriate. Service interruptions or failure to achieve the SLAs will not be subject to penalty in the event of noncompliance with the above.

(Optional) Out of Band (OOB) Hardware (Managed Device)

For purposes of Managed Device maintenance and troubleshooting, Dell SecureWorks can provide an optionally-orderable element of the Service – equipment that will enable the SOC to remotely and securely connect to the Managed Device.

Dell SecureWorks can provide equipment to be attached to the POTS line and/or additional IP address in order to provide OOB access for Customers who choose this option. Upon mutual agreement by the parties, Customer's existing OOB access option may be used where appropriate. **IMPORTANT:** Service interruptions or failure to achieve the SLAs will not be subject to SLA credit in the event of noncompliance with the above.

Timelines

The following Managed Device, location, and time-frame assumptions are used for purposes of providing a standard project-based timeframe for a Provisioning project plan:

- 1-4 Managed Devices total.
- 1 physical location.
- Dependencies external to Dell SecureWorks such as Customer-provided information and shipping carrier responsibilities are not included within the provisioning estimate.

Based on these assumptions, Dell SecureWorks can generally provision the Managed Device(s) within five (5) weeks, not including the time required for Customer activities.

Advanced Malware Protection

The Service delivers threat protection against advanced malware threats by providing two types of capability: *Inbound Malware Detection and Response*, and *Infection Detection and Response*. The Service is specifically designed to detect, block, and alert on inbound malware, and to also detect and respond to existing malware infections that have evaded preventative security systems.

Inbound Malware Detection and Response

The Service utilizes malware detection technology deployed in the Customer network to detect and respond to inbound malware targeting the Customer through email attachments and web traffic.

Email Attachments

The Service can protect against inbound malware in unencrypted email attachments provided Customer has acquired the appropriate supported product for email protection. Attachments are inspected and executed in real time, observed for inappropriate/malicious behavior, and, if necessary, alerted on and quarantined.

Web Traffic

The Service can protect against inbound malware in unencrypted web content provided Customer has acquired the appropriate supported product for web protection. Web content is inspected in real time, observed for inappropriate/malicious behavior, and, if necessary, alerted on and blocked.

"Phishing" Attack Correlation

The Service can correlate "phishing" attacks by relating the initial email message with a phishing link to the malicious web content pointed to by the link, provided Customer has acquired the appropriate supported products for this correlation.

Infection Detection and Response

The Service uses malware detection technology deployed in the Customer network to automatically discover infections by monitoring network traffic on endpoint devices; for example, PC's, laptops, mobile devices, servers, and files. The Service monitors egress, proxy, and DNS traffic to identify suspicious behaviors that would indicate the presence of malware and criminal command and control. It identifies active, hidden threats by detecting various behaviors indicative of criminal/malware activity including:

- Communications to Suspicious Destinations
 - DNS queries for suspicious or known malicious domains
 - Connection attempts to suspicious or known malicious destinations by Customer network Egress or Proxy
 - Suspicious communications to new destinations from within your network
- Suspicious Communication Content
 - Suspicious or zero-day malware downloads
- Suspicious Network Communication Behaviors
 - Connection behavior that seems more automated than human-driven
 - Domain fast fluxing activity (clusters of NXDOMAIN queries)

These observations are automatically correlated with advanced cyber threat intelligence to positively identify the specific threat type, provide attribution to the criminal operator, and determine the likelihood of infection.

The Counter Threat Platform (as defined below) can aggregate and correlate security events from the Advanced Malware Protection appliance. This industry-leading Dell SecureWorks-developed technology processes log and alert information to identify and present security events of interest to our Analysis team. These security experts then conduct further analysis, and once a threat has been discovered, Dell SecureWorks notifies Customer personnel through the creation of a Security Incident ticket, a telephone call, and/or other notification mechanisms in accordance with the notification/escalation procedures selected by the Customer in advance. System access call profiles for malware samples can be captured for further analysis. Customers can view security events and perform incident workflow through the Counter Threat Portal.

Counter Threat Platform Customer Portal

Dell SecureWorks provides Customer with access to the Dell SecureWorks Counter Threat Platform Customer Portal (the "Portal"). The Portal may only be accessed by the named individuals specified by Customer during the Information Gathering phase and identified on the Service Initiation Form (SIF), or by individuals who have been added to the list of named individuals after Service Activation. All information received by Customer through the Portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization without written authorization from Dell SecureWorks.

24x7 SOC Access

Customer may contact the Dell SecureWorks Security Operations Center (SOC) 24 hours a day, 7 days a week, and 365 days a year through the portal or telephone.

- The SOC can provide assistance with troubleshooting possible Managed Device-related incidents.

- The SOC can change contact information or reschedule change times.
- The SOC cannot provide general consulting advice that does not directly pertain to the results of the Service.

Managed Device Uptime Monitoring

Dell SecureWorks must be able to connect to the Managed Device through a network address translation module on the CTA.

Dell SecureWorks will perform uptime monitoring of the device. Dell SecureWorks monitors uptime via periodic polling of the Managed Device. If a failed or negative response is received from periodic polling checks, an automatic alert is sent to Dell SecureWorks, which then generates a ticket.

Dell SecureWorks will perform certain manual checks before notifying Customer within the time specified in the SLA. After Customer notification, Dell SecureWorks may perform further troubleshooting or remediation steps after the root problem is identified.

- If the root problem lies with the Managed Device, Dell SecureWorks will attempt to bring the Managed Device back up. Dell SecureWorks will work with Customer's designated point of contact by phone to address any device-related problems.
- If the root problem is Customer related, such as a network change, outage, or Customer-managed device, Dell SecureWorks will provide Customer with any available troubleshooting information, but Dell SecureWorks is not responsible for troubleshooting issues that do not directly relate to the Managed Device, Dell SecureWorks' collection device, or network.

Upgrade and Patch Management

Dell SecureWorks monitors all vendors represented on Dell SecureWorks' approved platforms list for release activities related to software patches and upgrades. As security related software patches and upgrades are released, Dell SecureWorks assesses the applicability of each release to Customer's environment. Dell SecureWorks will work with Customer to schedule any necessary remote upgrades.

Patches are applied at no additional charge. Customer-Owned Equipment upgrades are implemented by Dell SecureWorks as part of the selected service as long as the following conditions apply:

- The upgrade can be performed remotely, either independently or with a minimal amount of on-site assistance by Customer.
- The upgrade does not require a change to underlying hardware on which Customer-Owned Equipment is deployed.
- A single upgrade does not require more than 2 person-hours of Dell SecureWorks' time. If additional time is required, it will be performed on a time and materials basis pursuant to a separate Statement of Work.

Dell SecureWorks will bill Customer for all work beyond the allocated 2 hours and for any work that requires a Dell SecureWorks employee to travel to Customer's site. If the upgrade requires any additional licensing or maintenance fees, Customer will be responsible for these fees.

In cases where support for a particular product or product version is being discontinued by the vendor or by Dell SecureWorks, Dell SecureWorks will communicate new platform migration options. To be assured of uninterrupted service, Customer must complete the migration process within 60 days. Customer bears any costs relating to procuring new hardware or components and to re-provisioning any Managed Devices.

SLAs do not apply during maintenance work. In addition, SLAs cannot be guaranteed if Customer does not make the changes required by Dell SecureWorks or if Customer prevents Dell SecureWorks from making the changes it notifies Customer are necessary for continued service.

Implementation of Replacement Hardware and Hardware Upgrades

As part of the Service, Dell SecureWorks will deliver initial implementation services for replacement hardware for Managed Devices declared by the vendor as defective. It is the Customer's responsibility to obtain replacement Managed Devices. Customer-provided replacement hardware must be the same vendor make and model as the defective Managed Device.

In our discretion, Dell SecureWorks may agree to perform same-vendor hardware upgrades for Customer. Upgrades due to Customer's wish to upgrade the vendor model or product end of life (EOL), etc. will incur additional fees.

Management Console

This section describes Dell SecureWorks' service delivery commitments associated with managing a management console located at a Customer site (On Premise Management Console), which may be part of the Customer's malware protection technology set. Any other service requests associated with managing such a management console are out-of-scope. Upon request, Dell SecureWorks may provide out-of-scope technical support on a time and materials basis pursuant to a separate Statement of Work.

Two different service delivery models are available for management consoles:

Fully Managed

In this scenario, Customer provides Dell SecureWorks with a privileged application account as well as a privileged operating system account to the management console. Customer retains no operating system or application access to the Managed Devices. Customer must maintain a valid vendor maintenance support.

Co-Managed

In this scenario, Customer provides Dell SecureWorks with a privileged application account as well as a privileged operating system account to the management console. Customer retains administrative operating system and application access to the Managed Devices. Customer must maintain a valid vendor maintenance support.

Application Upgrades

In either management scenario, Dell SecureWorks may perform the following in addition to configuration and troubleshooting of the Dell SecureWorks managed devices:

- **Application Upgrades** – Application upgrades will be required from time to time in order to maintain vendor support and resolve existing application issues. Dell SecureWorks will notify Customer of an upcoming On-Premise Management Console upgrade. If Dell SecureWorks deems the upgrade is of significant risk, Dell SecureWorks may request that a technically-able representative be available during the upgrade, and will work with the Customer to establish a mutually acceptable maintenance window. If the Customer performs an application upgrade, Dell SecureWorks must be notified at least 72 hours ahead of a console upgrade in order to ensure that service continuity is maintained.

Change Management

Customer may submit a standard change request to Dell SecureWorks by telephone or the Portal. Dell SecureWorks requires that the change request is made by an authorized Customer contact. Dell SecureWorks will contact Customer to clarify unclear requests as needed.

Advanced Event Analysis and Threat Context

Upon customer request, Dell SecureWorks will perform a comprehensive analysis of the alert and subsequent samples submitted, and deliver a detailed report with the following information:

- Alert Details/Background
 - Original alert data, source host/IP, date/time, DSWRX ticket numbers and other pertinent background information
- Technical Details (as relevant and accessible as it relates to the given malware sample)
 - Malware family
 - Noted system or OS changes
 - Domain and Host names related to event
 - Other identifiable threat indicators
- Threat Context (Where applicable and available for the particular malware sample)
 - Leverage Dell SecureWorks Threat Indicator Management System (TIMS) to perform correlation and link analysis
 - Report on previously seen versions of the malware and it's prevalence
 - Provide additional details and threat context as available
- Recommendations
 - Suggested actions for Customer to take to resolve the event and/or prevent future occurrence

To provide Threat Context, Dell SecureWorks proactively correlates multiple intelligence sources for network and host threat indicators, including:

- Indicators from Dell SecureWorks global security monitoring data
- Indicators from collected malware processed by our three-stage automation process designed to extract network and host indicators
- Indicators from our Advanced Persistent Threat research to include network and host indicators from known APT infrastructure and associated tradecraft
- Indicators from botnets monitored by the security experts in our Counter Threat Unit research team
- Indicators from underground threat actor chatter as monitored by Dell SecureWorks
- Indicators from public dump sites such as pastebin.com

When Customer is alerted to an AMP event, they will have the option to request Advanced Event Analysis and Threat Context on the event in consideration. Customer is limited to the following number of advanced analysis reports during the annual contract period:

- Appliances with a throughput of <=50 Mbps or <= 150K emails/day: 12 events
- Appliances with a throughput of 50-250 Mbps or 150K -300K emails/day: 18 events

- Appliances with a throughput of > 250 Mbps or > 300K emails/day: 24 events

Customer Directed Research for AMP Events

Customer retains a fixed block of 40 hours per year that can be applied towards additional, focused research on AMP events. Following receipt of an Advanced Event Analysis and Threat Context report, Customer has the option to engage the analysis consultant for a review of the findings and recommendations, or additional investigation into the threat. Hours spent delivering work is accrued in half-hour increments. Unused hours expire at the end of each service year.

Upon Customer request, malwares samples may be escalated to the Counter Threat Unit Research Team for human analysis and reverse engineering. CTU Research work effort will accrue against the retained hours at a rate of 2x.

Other (Out of Scope) Services

Any other services are out-of-scope. Upon request, Dell SecureWorks may provide out-of-scope technical support on a time and materials basis pursuant to a separate Service Order. Examples of such out-of-scope support include, but are not limited to:

- On-site installation and provisioning of Managed Device
- Integration of complementary products that are not managed by Dell SecureWorks; for example SIEM, GRC, network packet capture technologies
- Custom analysis and/or custom reports, except as defined above
- Configuration of any tunnel end point that is not terminated on a Dell SecureWorks-managed device
- Incident response and forensics, except as retained in a separate Statement of Work
- Security Best Practice Consulting

Customer Requirements

Customer agrees to perform the obligations and acknowledges and agrees that Dell SecureWorks' ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

Order and Delivery of Managed Devices

Customer is responsible for procuring and arranging delivery of Managed Devices, including replacement Managed Devices as necessary. For additional information regarding hardware purchases, please contact your Dell SecureWorks representative."

Return Merchandise Authorization (RMA) Process Responsibilities

Customer is responsible for initiating and fulfilling the RMA process with their 3rd party vendor in the event that the Hardware/Software being managed by Dell SecureWorks is determined to be in a failed or faulty state that requires replacement.

Hardware/Software

Dell SecureWorks' SLAs will not apply to platforms that are End of Life, End of Support, or are otherwise not receiving updates by the vendor.

Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance (including 3rd party hardware and software contracts) for the Customer-owned Managed Devices and connectivity to prevent network performance degradation and maintain communications between the Customer's contracted Managed Devices and Dell SecureWorks' Secure Operations Center or SOC.

Connectivity

Customer will provide access to Customer-premises and relevant appliance(s) and management console(s) necessary for Dell SecureWorks to manage and monitor the contracted Managed Devices. Customer will ensure that Managed Devices have Internet access to the vendor's malware protection cloud (cloud.fireeye.com) so that software updates may be downloaded in a timely fashion. Additionally, Customers should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Dell SecureWorks Customer portal. SLAs will not apply to Managed Devices that are experiencing Customer-caused connectivity issues.

Advance Notification of Management Console Upgrades

Customer must notify Dell SecureWorks at least 72 hours ahead of an On-Premise Management Console upgrade in order to ensure that service continuity is maintained.

Service Level Agreements

Service Level Matrix

SLA	Definition	SLA Credit
Availability	<p>Dell SecureWorks aims for high availability for the Service. This means high availability of the Portal to our customers subscribing to this Service as well as high availability of communications flow between our infrastructure and our customers monitored and managed environments.</p> <p>To attain this goal, Dell SecureWorks maintains communications availability to the Internet 99.9% of the time during any calendar month, excluding planned maintenance windows.</p> <p>"Communications availability" is defined as the ability for one of Dell SecureWorks' SOC's to transmit and receive TCP/IP packets between its networks and its upstream Internet Service Provider.</p> <p>In the event that this SLA is not met for a given calendar month, Customer shall be entitled to a monetary credit equal to 1/30th of the monthly rate paid for the Service(s) delivered during that calendar month. Dell SecureWorks makes no guarantee to availability or performance of the internet at large between Dell SecureWorks' customers to the internet. Dell SecureWorks' measuring of 99.9% is executed from multiple sites throughout the internet to the Dell SecureWorks SOC's.</p>	1/30 th of monthly fee of affected Service
Standard Change Request	<p>Change Requests identified as "Standard" will receive the following Service Levels:</p> <ul style="list-style-type: none"> Acknowledgement of change within one (1) business hour from the time stamp on the help desk ticket created by Dell SecureWorks Scheduling of the change window within six (6) hours of receipt of requirements from Customer Deployment of the change within four (4) hours of the scheduled change window 	1/30 th of monthly fee for Service for the affected Managed Device
All Other help desk Requests	<p>Standard help desk requests (applies to all non-change and non-incident tickets) submitted through the Dell SecureWorks Portal or by telephone will be subject to "acknowledgement" (either through the help desk ticketing system, email, or by telephone) of receiving the request within one (1) hour from the time stamp on the help desk ticket created by Dell SecureWorks.</p> <p>An acknowledgement to help desk requests classified as "Urgent" on the help desk ticket and verified by the SOC as "Urgent" will be sent (either through the help desk ticketing system, email or telephonically) within fifteen (15) minutes from the time stamp on the help desk ticket created by Dell SecureWorks.</p>	1/30 th of monthly fee for Service

Security Monitoring	<p>Customer shall receive a response (according to the escalation procedures defined in the Portal or in the manner pre-selected in writing by Customer, either through the help desk ticketing system, email, or by telephone) to security incidents within fifteen (15) minutes of the determination by Dell SecureWorks that given malicious activity constitutes a security incident. This is measured by the difference between the time stamp on the incident ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.</p> <p>A "security incident" is defined as an incident ticket that comprises an event (log) or group of events (logs) that is deemed high severity by the SOC in accordance with Dell SecureWorks' Event Handling Process (see Exhibit A). (The most up-to-date version can always be found in the Real-Time Events section of the Portal).</p> <p>Automatically created incident tickets (via correlation technology) and event(s) or log(s) deemed low severity will not be escalated, but will be available for reporting through the Portal.</p>	1/30 th of monthly fee for Service for the affected Managed Device
Active Health Monitoring	<p>Active health checks identifying the following conditions are subject to the coinciding SLAs below:</p> <p>Device Unreachable – 30 minute response (via phone, ticket or email) from identification of the Managed Device being unreachable. This is measured by the difference between the time stamp on the Managed Device unreachable ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.</p>	1/30 th of monthly fee for Service for the affected Managed Device
Advanced Event Analysis and Threat Context Reports	Advanced Event Analysis and Threat Context Reports will be delivered to the Customer within two (2) business days from the time the Customer makes the request in the Portal.	These reports will not count towards the total number of purchased reports.

Additional Service Rules, Regulations, and Conditions

- a. The MMAMP Service provides robust device management, security analysis, and performance monitoring to Customer. However, deployment of this Service in Customer's network does not achieve the impossible goal of risk elimination, and therefore Dell SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on Customer's network.
- b. Dell SecureWorks may schedule maintenance outages for Dell SecureWorks-owned equipment/servers, which are being utilized to perform the services, with 24-hours' notice to designated Customer contacts.
- c. The Service Levels set forth herein are subject to the following terms, conditions, and limitations:
 - i. The Service Levels shall not apply during scheduled maintenance outages and, therefore, are not eligible for any Service Level credit.
 - ii. The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Dell SecureWorks from providing the Service or delivering the Service Levels or managed service descriptions, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any

managed hardware or software devices by Customer, its employees, agents, or third parties acting on behalf of Customer.

- iii. Furthermore, the Service Levels shall not apply to the extent Customer does not fulfill and comply with its obligations and interdependencies set forth within this SLA (see "Customer Requirements" above). The obligations of Dell SecureWorks to comply with the Service Levels with respect to any incident response or help desk request are also interdependent on Dell SecureWorks' ability to connect directly to Customer's Managed Devices on Customer's network through an authenticated server in the Dell SecureWorks Secure Operations Center.
- d. Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Dell SecureWorks of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Dell SecureWorks within thirty (30) days of such failure. Dell SecureWorks will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the Agreement, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.

Exhibit A – Dell SecureWorks' Event Handling Process

Event Handling Process

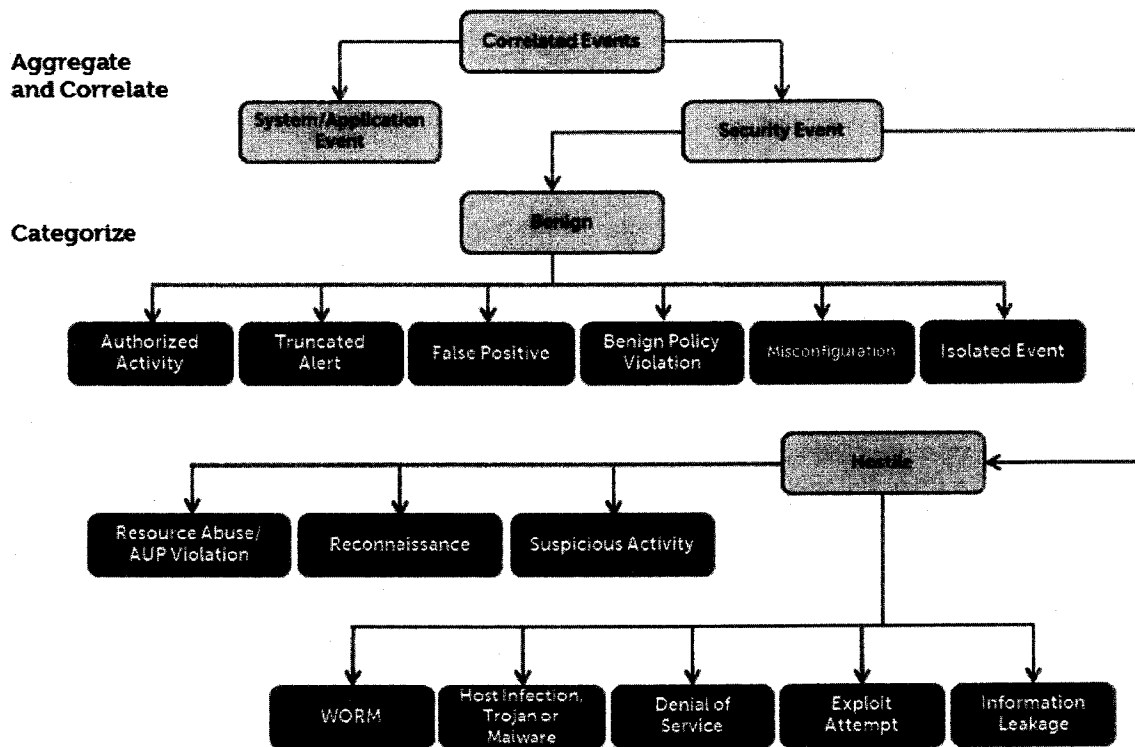


Exhibit B – Dell SecureWorks Maintenance Program Terms and Conditions

- Dell SecureWorks agrees, subject to the terms and conditions of your separate master service agreement or security services schedule (and as further set forth below), to replace Dell SecureWorks iDevices that are not properly functioning adequately due to ordinary wear and tear, malfunctions, inadequate available memory, or obsolescence. Replacement iDevices may be new or refurbished. These terms and conditions do not apply to Managed Devices as defined in this Service Description, including security products manufactured by FireEye.
- iDevices subject to this Program may include the Dell SecureWorks' CTA, iSensor IPS/IDS appliances, Enterprise iSensor IPS/IDS appliances, LogVault appliance, Inspector, SDA, SYSLOG Aggregator, log collection devices, and/or SNORT IDS device.
- If Customer is purchasing an iDevice, the following terms apply:
 1. Mere purchase by Customer of an iDevice does not subject the same to this Program unless: (a) such iDevice is expressly specified in a written Dell SecureWorks Service Order or Service Agreement signed by an authorized officer of Dell SecureWorks and (b) Customer's payment of all maintenance fees is made when due.
 2. Customer may elect to participate in the maintenance program only at the time of purchase of the Dell SecureWorks iDevice. If, at any time after the purchase of the Dell SecureWorks iDevice, Customer wishes to participate in this Program, it must agree to pay all fees that would have been billed since the actual date of purchase of the iDevice.
- The charges for the maintenance program only cover replacement of Dell SecureWorks iDevices. Any performance, damage, repair and/or other warranty issues, or claims with respect to non-Dell SecureWorks-branded iDevices must be addressed with the applicable OEM manufacturer.
- Dell SecureWorks' obligation to comply with the foregoing is conditioned upon, and subject to, the assistance and availability of Customer's onsite personnel for assistance in the: (x) diagnosis and troubleshooting of problems with existing iDevices and (y) replacement and installation of any new iDevice all in compliance with your master service agreement or services schedule.
- Furthermore, Dell SecureWorks will not replace Dell SecureWorks iDevices returned by Customer that are no longer performing on account of unauthorized use, physical damage, or misuse or abuse of the products, as determined by Dell SecureWorks in its sole discretion, including, but not limited to, any of the following circumstances:
 1. Damage due to lightning or other climate problems (including, but not limited to, exposure to excessive light, heat, flooding, and the like);
 2. Opening of iDevices by any person other Dell SecureWorks authorized personnel;
 3. Unauthorized loading or modification of software on or other reprogramming of the iDevice;
 4. Unauthorized linking of the iDevice with other Customer equipment or systems;
 5. Cracks in iDevices, dents to chassis or apparatus, or other damage caused by dropping of iDevice or other mishandling, misuse, or abuse;
 6. Presence of liquids (or residue there from) or the excessive presence of other extraneous materials inside the iDevice (including, but not limited to, dust, hair, dirt, or grime);
 7. Inability to mount the iDevice;
 8. Improper powering down of the iDevice.

- Dell SecureWorks shall bill Customer, and Customer shall be liable, for iDevices: (i) damaged due to Customer's misuse or abuse, or (ii) no longer performing adequately due to unauthorized use, physical damage, misuse, or abuse of the iDevices by Customer.
- Customer is strongly encouraged to purchase spare equipment to maintain fail-over iDevices within countries located outside of the United States.

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 6: Managed and Monitored IPS Service Description and Service Level Agreements

Managed and Monitored IPS Service Description and Service Level Agreements

This Service Description and Service Level Agreement and the attached appendices (collectively, the "Service Description") is provided for the customer ("Customer" or "you") and the Dell entity identified in the service order ("Service Order") executed by Customer and such Dell entity for the purchase of this Service (as defined below) ("Dell SecureWorks"). This Service is provided in connection with Customer's separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security services. In the absence of either a master services agreement or security services schedule, the Services performed under this Service Description are governed by and subject to the terms and conditions of the Dell SecureWorks Master Services Agreement, available at www.Dell.com/Securityterms which is incorporated by reference in its entirety herein (the "MSA").

Service Overview

The Dell SecureWorks® Managed and Monitored Intrusion Prevention ("MMIPS") Service (the "Service") provides proactive administration of your Intrusion Prevention ("IPS") infrastructure 24 hours a day, 7 days a week, and 365 days a year. Dell SecureWorks' certified security experts will perform all activities necessary to keep these devices operating at peak performance.

Service Description

Dell SecureWorks' proprietary platform provides the foundation for delivery of our managed security services. The following service components are included with the managed and monitored intrusion detection and prevention service unless otherwise mentioned:

Policy Management

Dell SecureWorks manages the policy on the device. The policy will be tuned so that each signature is classified by action and by severity level. Major Events are events that Dell SecureWorks has a high degree of confidence are a significant risk to Customers. These events may require immediate notification and swift resolution by Dell SecureWorks or Customer. Minor Events are events that Dell SecureWorks does not believe pose an immediate threat or risk. Dell SecureWorks determines which events belong in the Major Event category through the use of signature priorities, algorithms, event correlation, and Dell SecureWorks' professional judgment. All other security incidents are considered Minor.

Blocking traffic creates the risk of potential disruption to Customer's business. Dell SecureWorks is not responsible for negative impacts to Customer as a result of network traffic blocked by device. Dell SecureWorks will work with Customer to tune the policy during the initial tuning period.

Customers may request that a signature be blocked, unblocked, or reprioritized by calling Dell SecureWorks or opening a ticket in the Customer portal.

Initial Policy Tuning

Upon service activation, Dell SecureWorks applies one baseline policy to each device. Dell SecureWorks then tunes the policy to Customer's environment during the thirty (30) day tuning period which begins on the Service Commencement Date. During this tuning period, Dell SecureWorks works with Customer to determine the action and severity applied to signatures.

Policy Maintenance

Policies are updated regularly as updates are released by vendors and reviewed by Dell SecureWorks. If applicable, critical signatures that Dell SecureWorks recommends for blocking will be set to simulated block and pushed to the device in the next policy update cycle. These signatures can be tuned to block on a one-off basis by calling Dell SecureWorks or via the Customer portal. Additionally, Customer can pre-approve all signatures for blocking in which case all new blocking signatures will be pushed to the device in block mode without additional Customer approval.

If supported by the device, Dell SecureWorks can configure the device to fail open or closed, depending on Customer preference. In the event of device failure, if the device configured to fail open, no traffic will be blocked; if configured to fail closed, all traffic will be blocked.

Health and Uptime Monitoring

Dell SecureWorks' proprietary platform provides active and passive health checks on managed and monitored devices. Active checks are performed only on devices being managed to obtain system level performance information. Passive checks are performed using event flow trending technology to detect loss of log collection from managed and monitored devices. Device health information and ticketing workflow is displayed in the Portal for Customer consumption.

Dell SecureWorks must be able to connect to the device via the Internet using ICMP and SSH.

Dell SecureWorks monitors uptime via periodic polling of the device. If a failed or negative response is received from periodic polling checks, an automatic alert is sent to Dell SecureWorks, which then generates a ticket.

Dell SecureWorks will perform certain manual checks before notifying Customer within the time specified in the SLA. After Customer notification, Dell SecureWorks may perform further troubleshooting or remediation steps after the root problem is identified.

- If the root problem lies with the device managed by Dell SecureWorks, Dell SecureWorks will attempt to bring the device back up. Dell SecureWorks will work with Customer's designated point of contact via phone to address any device related problems.
- If the root problem is Customer related, such as network change, outage, or Customer-managed device, Dell SecureWorks will provide Customer with any available troubleshooting information, but Dell SecureWorks is not responsible for troubleshooting issues that do not directly relate to the device, Dell SecureWorks client premise equipment, or Dell SecureWorks' network.

Security Event Monitoring

Device log data is gathered by the client premise equipment and transported to Dell SecureWorks. The data is parsed, normalized, correlated, and prioritized. The security events are categorized by Dell SecureWorks based on the severity level. Dell SecureWorks also performs additional analysis to determine whether the event is a false positive. Dell SecureWorks provides Customer with a description of the event and any contextual information. The event is also posted on the Customer Portal and made available for reporting. In depth analysis, incident response, forensics, and countermeasures are not included in this service.

Software Upgrade and Patch Maintenance

Dell SecureWorks monitors all vendors represented on Dell SecureWorks' approved platforms list for release activities related to software patches and upgrades. As security related software patches and upgrades are released, Dell SecureWorks assesses the applicability of each release to Customer's environment. Dell SecureWorks will work with Customer to schedule any necessary remote upgrades.

In cases where support for a particular product or product version is being discontinued by the vendor or by Dell SecureWorks, Dell SecureWorks will communicate new platform migration options. In order to be assured of uninterrupted service, Customer must complete the migration process within 60 days.

SLAs do not apply during maintenance work. SLAs cannot be guaranteed if Customer does not make the changes required by Dell SecureWorks or if Customer prevents Dell SecureWorks from making the changes it notifies Customer are necessary for continued service.

Other Services

Any other services are out-of-scope. Upon request, Dell SecureWorks may provide out-of-scope technical support on a time and materials basis pursuant to a separate SOW. Examples of such out-of-scope support include:

- On-site installation and provisioning of device
- Analysis of minor events
- Integration of complementary products that are not managed by Dell SecureWorks (e.g., antivirus software; web reporting software).
- Development of customized signatures
- Custom analysis and/or custom reports
- Forensics

Add-On Options

The following services are not included in the standard Managed and Monitored Intrusion Prevention Service offering but are available from Dell SecureWorks at an additional cost.

High Availability

As an optional service upgrade, Dell SecureWorks offers a High Availability solution for intrusion prevention devices that natively support High Availability.

Management Console

This section describes Dell SecureWorks service delivery commitments associated with managing a management console located at a Dell SecureWorks site ('Hosted Management Console') or at a Customer site ('On Premise Management Console'). Any other service requests associated with managing a management console are out-of-scope. Upon request, Dell SecureWorks may provide out-of-scope technical support on a time and materials basis pursuant to separate SOW.

Hosted Management Console

In this scenario, management consoles are housed within a Dell SecureWorks data center. The service delivery model associated with Hosted Management Console is described below:

Fully Managed

In this scenario, Dell SecureWorks shall maintain exclusive administrative privilege to the management console and will manage all devices contained within the management console. Upon Customer request, read only access to the management console may be provided to the Customer. Customers who have read-only access to the hosted management console will be notified in advance of any work being performed on the management console.

Dell SecureWorks may perform the following:

- Console Backup and Restore

Dell SecureWorks will maintain hosted managed management console backups at a Dell SecureWorks site to rebuild the management console, in the event of a hosted managed management console failure.

- Application Upgrades

Dell SecureWorks will perform application upgrades from time to time in order to maintain vendor support and resolve existing application issues.

On-Premise Management Console

In this scenario, management consoles shall be housed at a Customer site. Two different service delivery models are associated with Hosted Management Consoles: Co-Managed and Access-Only.

Co-Managed

In this scenario, the Customer provides Dell SecureWorks with a privileged application account as well as a privileged operating system account to the management console. Customer retains administrative operating system and application access to the devices. Customer must maintain a valid vendor maintenance support.

Dell SecureWorks may perform the following in addition to policy rule and object modification, addition, deletions, troubleshooting for the Dell SecureWorks managed devices:

- Console Backup and Restore

Dell SecureWorks requires that the management console backups be stored and maintained by the Customer on a remote device at the Customer site.

Depending upon the vendor platform, Dell SecureWorks shall maintain On-Premise management console backups on the Dell SecureWorks client premise equipment. In the event of a remotely managed management console failure requiring a rebuild, Dell SecureWorks will work with the Customer to transfer a copy of the latest backup to the On-Premise management console.

- Application Upgrades

Application upgrades will be required from time to time in order to maintain vendor support and resolve existing application issues. Dell SecureWorks will notify Customer of a coming On-Premise management console upgrade. If Dell SecureWorks deems the upgrade is of significant risk, Dell SecureWorks may request that a technically-able representative be available during the upgrade and will work with the Customer to establish a mutually acceptable maintenance window. If the Customer performs an application upgrade, Dell SecureWorks must be notified at least 72 hours ahead of a console upgrade in order to ensure that service continuity is maintained.

Access-Only

In this scenario, the Customer will create Dell SecureWorks an application account with the necessary privileges to perform policy modifications, deletions, additions and installation of policies and objects for the Dell SecureWorks-managed devices. The Customer is responsible for ongoing maintenance, updates, backups, upgrades of the On-Premise management console. Customer must notify Dell SecureWorks at least five (5) days ahead of a console upgrade in order to ensure that the proper support is maintained.

Application Intelligence and Control

Dell SecureWorks can enable application control as per Customer's request. There are over 1200 applications supported within the device, therefore it is Customer's responsibility to specify all application control and application rule settings required. Dell SecureWorks will configure the device in accordance with the Customer's specifications.

Dell SecureWorks does not offer application debugging in the event of unexpected consequences from application control settings. Dell SecureWorks' responsibilities surrounding application control are limited to enabling or disabling the application control settings. At the time of initial deployment, by default, application intelligence and control is turned off.

User Control

This service enables control and monitor of user activity in the Customer network.

To perform user control, Customers must use Microsoft active directory LDAP servers. The system obtains the users and groups that can be used in access control rules from Active Directory, and also ties users to IP addresses with the logins reported by the user agents installed on Active Directory servers. The user agent works in conjunction with the managed IPS device to gather user data. The user agent is also essential to implementing user access control.

Dell SecureWorks managed services helps customers to setup a user agent on the management console and configure the management console to connect to a user agent. Dell SecureWorks will also provide appropriate instructions to Customers to configure user agents on Microsoft active directory servers. Upon customer's request, Dell SecureWorks can control or monitor appropriate user activity in the Customer network. Service does not cover installation or continued management or monitoring of user agents installed on non-SecureWorks managed devices.

Advanced Malware Protection

The Service is specifically designed to detect and block malware infected files attempting to enter or traverse the network. The service also offers continuous analysis and subsequent retrospective alerting of infected files in the event malware determination changes after initial analysis.

In addition to Health Monitoring, Upgrade and Patch Management and Change Management, Dell SecureWorks aggregates and correlates security events from the Advanced Malware Protection appliance. This industry-leading Dell SecureWorks-developed technology processes log and alert information to identify and present security events of interest to our Analysis team. These security experts then conduct further analysis, and once a threat has been discovered, Dell SecureWorks notifies Customer personnel through the creation of a Security Incident ticket, a telephone call, and/or other notification mechanisms in accordance with the notification/escalation procedures selected by the Customer in advance. Customers can view security events and perform incident workflow through the Counter Threat Portal.

CTU Countermeasures

CTU Countermeasures are provided as a part of premium managed IPS Service. These Countermeasures supplements the Sourcefire VRT signatures. CTU Countermeasures are derived via in-depth analyses of malware samples and comprehensive vulnerability analysis. Deploying these countermeasures on the IPS appliance increases the effectiveness of your managed IPS to block communications to known command and control centers. Customers subscribed to this service is offered expert installation and configuration support CTU countermeasures from SecureWorks SOC. SecureWorks SOC initiates CTU signature updates typically twice a week (Tuesday and Thursday).

SecureWorks SOC may initiate additional signature updates to address critical vulnerabilities as and when required.

Customer Requirements

Customer agrees to perform the obligations and acknowledges and agrees that Dell SecureWorks' ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

Hardware/Software Procurement

The Customer is responsible for purchasing the IPS hardware and software necessary for Dell SecureWorks to deliver the MMIPS Service. Additionally, the Customer is responsible for ensuring their hardware/software stays within the 3rd party vendors' supported versions. Dell SecureWorks' SLAs will not apply to platforms that are end of life, end of support or are otherwise not receiving updates by the vendor.

Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance (including third-party hardware and software contracts) for the Customer owned IPS and connectivity to prevent network performance degradation and maintain communications between the Customer's contracted intrusion prevention devices and Dell SecureWorks' security operations centers (Secure Operations Centers" or "SOC(s)").

RMA Responsibilities

The Customer is responsible for initiating and fulfilling the return materials authorization ("RMA") process with their third-party vendor in the event that the hardware/software being managed by Dell SecureWorks is determined to be in a failed or faulty state that requires replacement.

Connectivity

Customer will provide access to Customer-premises and relevant appliance(s) and management console(s) necessary for Dell SecureWorks to manage and monitor the contracted intrusion prevention devices. Additionally, Customers should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Dell SecureWorks Customer portal. SLAs will not apply to devices that are experiencing Customer-caused connectivity issues.

Service Level Agreements (SLAs)

Service Level Agreements Matrix

SLA	Definition	SLA Credit
Standard Change Request	<p>Change Requests identified as "Standard" will receive the following service levels:</p> <ul style="list-style-type: none"> Acknowledgement of receiving the change within 1 business hour from the time stamp on the ticket created by Dell SecureWorks. 	1/30 th of monthly fee for Service for the affected device
Security Monitoring	<p>Customer shall receive a response (according to the escalation procedures defined in the Customer portal or in the manner pre-selected in writing by Customer, either through the ticketing system, email, or by telephone) to security incidents within fifteen (15) minutes of the determination by Dell SecureWorks that given malicious activity constitutes a security incident. This is measured by the difference between the time stamp on the incident ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.</p> <p>A "security incident" is defined as an incident ticket that comprises an event (log) or group of events (logs) that is deemed high severity by the SOC in accordance with Dell SecureWorks' Event Handling Process (see Exhibit A). The most up-to-date version can always be found in the Real-Time Events section of the Customer portal).</p> <p>Automatically created incident tickets (via correlation technology) and event(s) or log(s) deemed low severity will not be escalated, but will be available for reporting through the Customer portal.</p>	1/30 th of monthly fee for Service for the affected device
Active Health Monitoring	<p>Active health checks identifying the following conditions are subject to the coinciding SLAs below:</p> <ul style="list-style-type: none"> Device Unreachable – 30 minute response (via phone, ticket or email) from identification of the device being unreachable. This is measured by the difference between the time stamp on the device unreachable ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation. 	1/30 th of monthly fee for Service for the affected device
CTU Countermeasures Update (applicable only for customers subscribed to premium managed IPS Service)	<p>Dell SecureWorks will evaluate all US-CERT Advisories announcing remote vulnerabilities to determine if signature creation is possible. If the content of a US-CERT advisory is suitable and sufficient to craft signatures, those signatures shall be created and an IPS device update shall be initiated within 48 hours.</p>	1/30 th of monthly fee for Service for the affected device

Signature Updates of 3rd Party Devices

The current Operational Service Level Objective (SLO) for deploying third-party vendor signature updates is 48 business hours from Dell SecureWorks' receipt of such signature sets from the applicable third-party vendor. Dell SecureWorks attempts to push out new third-party signature sets as quickly as possible, but also endeavors to mitigate Customer security/network impact and risk by first loading signature sets in our lab or test devices and attempting to validate there are no adverse impacts with the set loading.

Additional Service Rules, Regulations, and Conditions

- a. Dell SecureWorks MMIPS Service provides robust device management, security analysis, and performance monitoring to the Customer. Deployment of Dell SecureWorks' MMNFW Service does not achieve the impossible goal of risk elimination, and therefore Dell SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on Customer's network.
- b. Dell SecureWorks may schedule maintenance outages for Dell SecureWorks owned equipment/servers which are being utilized to perform the services with 24-hours' notice to designated Customer contacts.
- c. The Service Levels set forth herein are subject to the following terms, conditions, and limitations:
 - i. The Service Levels shall not apply during scheduled maintenance outages and therefore are not eligible for any Service Level credit. Dell SecureWorks shall not be held liable for any Service impact or Service Levels Agreements related to product configurations that are not supported by Dell SecureWorks within the customer's policy.
 - ii. The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Dell SecureWorks from providing the Service, delivering the Service Levels or managed service descriptions, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by the Customer, its employees, agents, or third parties acting on behalf of Customer.
 - iii. Furthermore, the Service Level's shall not apply to the extent Customer does not fulfill and comply with its obligations and interdependencies set forth within this SLA. The obligations of Dell SecureWorks to comply with the Service Levels with respect to any incident response or ticket request are also interdependent on Dell SecureWorks' ability to connect directly to the Customer devices on the Customer network through an authenticated server in the Dell SecureWorks Secure Operations Center.
- d. If the Customer has purchased iDevice maintenance for a specific iDevice and such iDevice is not functioning properly, Dell SecureWorks will troubleshoot and, if necessary, replace such iDevices in accordance Exhibit B – Dell SecureWorks Maintenance Program Terms and Conditions.
- e. Monthly recurring cost may increase, should actual throughput utilized by the customer exceed the throughput customer has subscribed to. Dell SecureWorks reserves the right to audit the service on a quarterly basis and adjust service fees appropriately. Dell SecureWorks may adjust service fees quarterly to reflect actual service utilization.
- f. Customer will receive credit for any failure to meet the Service Levels outlined above within thirty (30) days of notification by Customer to Dell SecureWorks of such failure. In order for



Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Dell SecureWorks within thirty (30) days of such failure. Dell SecureWorks will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the Agreement, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.

Exhibit A – Dell SecureWorks' Event Handling Process

Event Handling Process

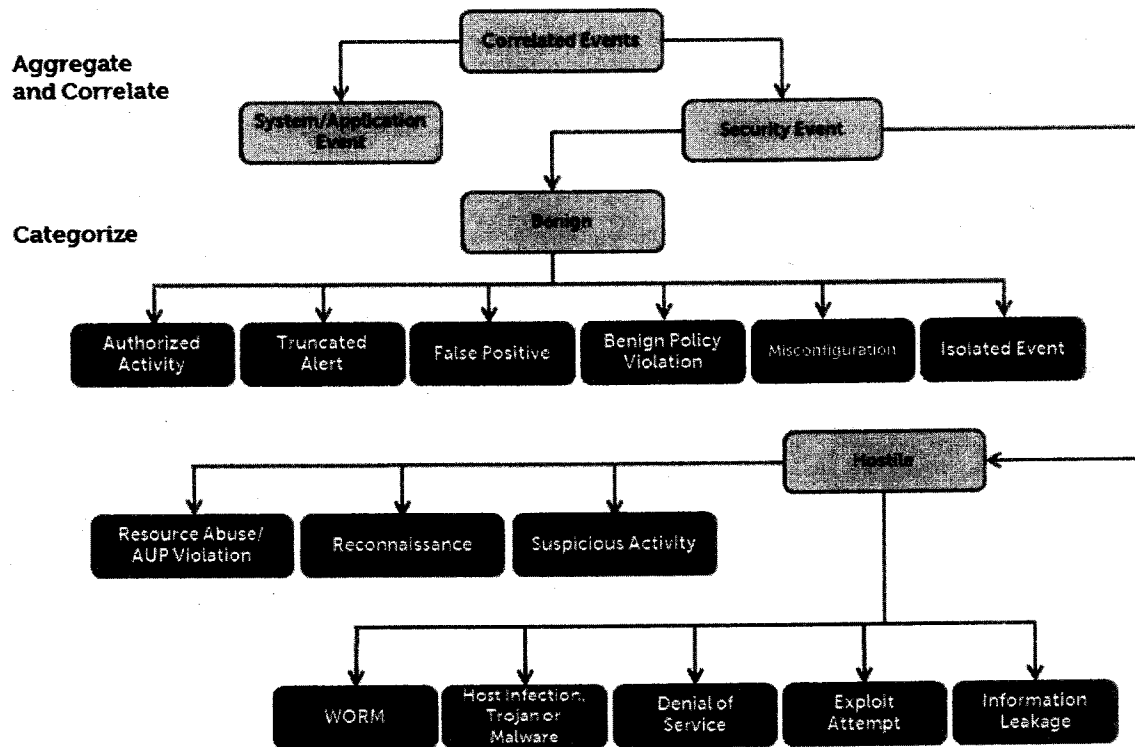


Exhibit B – Dell SecureWorks Maintenance Program Terms and Conditions

- Dell SecureWorks agrees, subject to the terms and conditions of your separate master service agreement or security services schedule (and as further set forth below), to replace Dell SecureWorks iDevices that are not properly functioning adequately due to ordinary wear and tear, malfunctions, inadequate available memory, or obsolescence. Replacement devices may be new or refurbished.
- iDevices subject to this Program may include the Dell SecureWorks' Counter Threat Appliance (CTA), iSensor, LogVault appliance, Inspector, SDA, SYSLOG Aggregator, log collection devices, and/or SNORT IDS device.
- If Customer is purchasing an iDevice, the following terms apply:
 1. Mere purchase by Customer of an iDevice does not subject the same to this Program unless: (a) such iDevice is expressly specified in a written Dell SecureWorks Service Order or Service Agreement signed by an authorized officer of Dell SecureWorks and (b) Customer's payment of all maintenance fees is made when due.
 2. Customer may elect to participate in the Program only at the time of purchase of the Dell SecureWorks iDevice. If, at any time after the purchase of the Dell SecureWorks iDevice, Customer wishes to participate in this Program, it must agree to pay all fees that would have been billed since the actual date of purchase of the iDevice.
- The charges for the Program only cover replacement of Dell SecureWorks iDevices. Any performance, damage, repair and/or other warranty issues, or claims with respect to non-Dell SecureWorks-branded iDevices must be addressed with the applicable OEM manufacturer.
- Dell SecureWorks' obligation to comply with the foregoing is conditioned upon, and subject to, the assistance and availability of Customer's onsite personnel for assistance in the: (x) diagnosis and troubleshooting of problems with existing iDevices and (y) replacement and installation of any new iDevice all in compliance with your master service agreement or services schedule.
- Furthermore, Dell SecureWorks will not replace Dell SecureWorks iDevices returned by Customer that are no longer performing on account of unauthorized use, physical damage, or misuse or abuse of the products, as determined by Dell SecureWorks in its sole discretion, including, but not limited to, any of the following circumstances:
 1. Damage due to lightning or other climate problems (including, but not limited to, exposure to excessive light, heat, flooding, and the like)
 2. Opening of iDevices by any person other Dell SecureWorks authorized personnel
 3. Unauthorized loading or modification of software on or other reprogramming of the iDevice
 4. Unauthorized linking of the iDevice with other Customer equipment or systems
 5. Cracks in iDevices, dents to chassis or apparatus, or other damage caused by dropping of iDevice or other mishandling, misuse, or abuse
 6. Presence of liquids (or residue there from) or the excessive presence of other extraneous materials inside the iDevice (including, but not limited to, dust, hair, dirt, or grime)
 7. Inability to mount the iDevice
 8. Improper powering down of the iDevice
- Dell SecureWorks shall bill Customer, and Customer shall be liable, for iDevices: (i) damaged due to misuse or abuse, or (ii) no longer performing adequately due to unauthorized use, physical damage, misuse, or abuse of the iDevices.

Managed Services in a Virtual Environment

Service Description Addendum

Definitions

This section details Dell SecureWorks' responsibilities associated with managing a Virtual Security Appliance ("VSA") delivering security services inside a virtual environment.

Virtualization includes various methods by which hardware resources are abstracted to allow multiple virtual machine ("VM") instances to share a common hardware platform. Key terms associated with virtualization used in this document are defined below:

- **Host** – Virtual machine host server that provides computing resources, such as processing power, memory, disk, and network I/O
- **Guest** – Separate and independent instance of operating system and application software that run on the Host
- **Hypervisor** – Virtual machine monitor that isolates each Guest from another, enabling multiple Guests to reside and operate on the host simultaneously
- **Virtual Security Appliance** – Software implementation of a security device (e.g. a Firewall, Intrusion Detection System) that executes programs like a physical machine

Dell SecureWorks' responsibilities associated with management of a virtual environment are limited to the VSAs running as Guests and actions performed on the Guest OS and configuration. Dell SecureWorks managed security services and SLAs available to VSAs running as a Guest are equivalent to those of the services in a non-virtualized (physical) environment.

Dell SecureWorks is not responsible for managing any aspects of operations related to hardware, Host, or Hypervisor on which a Guest instance managed by Dell SecureWorks is running.

Customer Requirements

Customer agrees to perform the obligations and acknowledges and agrees that Dell SecureWorks' ability to perform its obligations and its liability under the SLAs are dependent upon Customer's compliance with the following:

Provisioning & Maintenance

Maintenance of the Guest VM including provisioning, VM snapshot backup, and restoration of the Guest image as well as the underlying Hypervisor to provide inband management access for Dell SecureWorks must be performed by the Customer. The Guest OS must have a valid license for support. Dell SecureWorks is not in a position to provide any assistance without inband access to the Guest OS and without a valid license.

VSA Upgrades

Upgrade is limited to the Guest OS; Customer must resolve inband access issues in case of loss of connectivity for Dell SecureWorks management.

VSA Backups

Dell SecureWorks will back up Guest device configurations. It is the Customer's responsibility to backup and maintain the Guest (OVF) image. In the event of a Guest system requiring a rebuild, Dell

SecureWorks will restore the prior device configurations once the Customer restores the Guest and brings it back online.

VSA Health

To perform health checks on the virtual security appliance, Dell SecureWorks must be able to connect to the device via the Internet using Internet Control Message Protocol ("ICMP") and Secure Shell ("SSH"). The virtual security appliances are always assumed to be powered on, and any disappearance of the appliance from the network is considered a failure.

Dell SecureWorks will perform uptime monitoring of the device using periodic polling of the device. If a failed or negative response is received from periodic polling checks, an automatic alert is sent to Dell SecureWorks, which then generates a ticket. Health Monitoring is limited to appropriate application running as Guest OS. Dell SecureWorks does not perform health monitoring of hypervisor or the underlying hardware.

Out-of-Scope Services in a Virtual Environment

The following points are considered out-of-scope for this service:

- Restoring the VM image backups
- Troubleshooting issues at the Hypervisor level
- Troubleshooting performance issues not directly related to Guest OS such as hardware, hypervisor, or host-level issues

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 7: Monitoring Service Description and Service Level Agreements

Monitoring Service Description and Service Level Agreements

This Service Description and Service Level Agreement ("Service Description") describes the Service (as defined below) being provided to you ("Customer" or "you") by the Dell entity identified in the service order ("Service Order") executed by Customer and such Dell entity for the purchase of this Service. The Dell entity identified in the Service Order hereafter shall be collectively referred to as "Dell SecureWorks". This Service is provided in connection with Customer's signed Service Order and separate signed master services agreement or security services schedule that explicitly authorizes the sale of managed security and consulting services. In the absence of either a master services agreement or security services schedule, the Services performed under this Service Description are governed by and subject to the terms and conditions of the Dell SecureWorks Master Services Agreement, available at <http://Dell.com/Securityterms> which is incorporated by reference in its entirety herein (the "MSA").

Service Overview

The Dell SecureWorks® Security Monitoring service (the "Service") consists of Dell SecureWorks' monitoring of the contracted Customer-owned security device(s) ("Devices") as specified on the Service Order and provides Customer with real-time, security event analysis and response across Customer's security and critical infrastructure 24 hours a day, 7 days a week, 365 days a year. This Service combines Dell SecureWorks' advanced Counter Threat Platform ("CTP") with an expert team of security analysts to deliver strong security and compliance value to our customers.

Detailed Description

Dell SecureWorks' team of security experts will perform security analysis and passive health monitoring as set forth below.

Service Features

Feature	Description
Portal access	Dell SecureWorks proprietary Counter Threat Platform customer portal ("Portal") provides ticketing workflow management for incident management and other secure operations center ("SOC") interaction. The Portal also provides real-time visibility and reporting of Customer security events and associated incidents.
SOC access	Customer may contact the SOC 24 hours a day, 7 days a week, and 365 days a year through the Portal or by telephone. Inbound telephone calls to the SOC from Customer will result in the creation of a ticket. Receipt of each ticket will be acknowledged in accordance with the service level agreement outlined in the Service Level Agreements section of this Service Description.
Event monitoring, analysis and notification	Provides 24 hours a day, 7 days a week, and 365 days a year security event monitoring, analysis and notification.
Device health monitoring	Provides monitoring of Device health 24 hours a day, 7 days a week, and 365 days a year.

Service Activation

Service activation ("Service Activation") consists of three phases: information gathering, Counter Threat Appliance ("CTA") deployment (when applicable), and Device provisioning and installation.

Service Activation begins once the signed Service Order is received and ends with the activation of the Service.

Service Activation is dependent on a number of factors, such as the number of Devices, the number of applications, the number of physical sites, the complexity of the network, Customer requirements, and the ability of Customer to provide Dell SecureWorks with requested information within a mutually agreed-upon timeframe. Dell SecureWorks does not provide SLAs for completing Service Activation within a specified period of time.

Information Gathering

Once contracted for this Service, Dell SecureWorks will provide Customer with a Service Initiation Form ("SIF") to be completed and returned by Customer to Dell SecureWorks. Upon Dell SecureWorks' receipt of the completed SIF, Dell SecureWorks will schedule a conference call to review the SIF and other relevant information with Customer.

CTA Deployment (when applicable)

The CTA Deployment phase begins upon the completion of the Information Gathering phase described above.

The Counter Threat Appliance ("CTA") is a Dell SecureWorks-proprietary appliance that may be used in the secure delivery of the Service for health/security event acquisition and transport.

Using data gathered during the information gathering phase, Dell SecureWorks will determine whether CTAs are required. If so, Dell SecureWorks will then determine how many CTAs are necessary and the appropriate deployment location(s) within Customer's environment. For Services requiring the use of the CTA, Customer is responsible for ensuring that the implementation site or cloud service provider complies with Dell SecureWorks' physical/environmental requirements which such requirements shall be provided to Customer.

If changes to Customer's existing network architecture are required for Service implementation, Dell SecureWorks will communicate these changes to Customer.

Dell SecureWorks reserves the right, in its reasonable discretion, to utilize one or more CTAs deployed in a Dell SecureWorks data center ("hosted CTA") to communicate with Devices that Dell SecureWorks is monitoring, in lieu of deploying CTA(s) for use directly in Customer's network. In such a case, the terms and conditions pertaining to CTA deployment do not apply.

Service interruptions or failure to achieve the SLAs (as defined herein) will not be subject to penalty in the event of Customer's non-compliance with the above CTA deployment guidelines.

Service Provisioning and Installation

The Service Provisioning and Installation phase begins upon the completion of the Information Gathering and CTA Deployment phases described above.

Service Provisioning and Installation is performed in the following manner:

- New Customer Devices to be deployed are shipped directly to Dell SecureWorks for configuration and subsequent shipment to Customer location.
- Existing Customer-owned contracted Devices in use are provisioned remotely with on-site support from Customer.

- Dell SecureWorks provides telephone support to the Customer contact at the implementation site during installation of all Customer premises Devices.
- Once Customer premise contracted Devices are in place, Dell SecureWorks accesses the Device(s) remotely and performs the remaining configuration and Service activation tasks which may require device downtime.

Dell SecureWorks schedules Service provisioning and installation in accordance with change management procedures communicated by Customer during the Information Gathering phase. Standard installations are performed during the hours of 9 am and 5 pm EST, Monday through Friday, and may be performed at other times for an additional fee.

Service Components

Dell SecureWorks' Counter Threat Platform ("CTP") provides the foundation for delivery of the Service. This Dell SecureWorks-developed technology facilitates health monitoring, security analysis, and Customer reporting.

Health Monitoring

The CTP uses event flow technology to detect devices that are not sending logs to CTP as expected. The SOC analyzes any event flow disruptions and escalates to Customer as necessary. Customer can access device health information and ticketing workflow in the Portal.

Security Event Monitoring

Security event data is sent to the CTA or hosted CTA depending on how the Service is architected. In either case, the security event data is parsed, normalized, correlated, and prioritized. All security events are categorized by Dell SecureWorks based on severity level.

When a Critical Event is detected, initial correlation, de-duplication, and false positive reduction is performed by the correlation engine. If the security event is confirmed as a critical event, a ticket is automatically generated. Dell SecureWorks then contacts Customer within the time specified in the relevant SLA. Dell SecureWorks also performs additional analysis to determine whether the security event is a false positive.

Dell SecureWorks provides Customer with a description of the security event and any contextual information via the Portal. The security event is posted on the Portal and made available to Customer for review and reporting. In-depth analysis, incident response, forensics, and countermeasures beyond policy changes to the Device or other Dell SecureWorks managed Device(s) are not included in this Service. Customer is able to purchase these areas of advanced support under a separate, signed Service Order or statement of work.

Security Event Reporting

The Portal provides a secure mechanism to create, customize, and access executive and technical level reports, as well as view and report on detailed and historical security event data. The Portal enables Customer to create both standard and customized reports that can be named, scheduled to run at regular or one-off intervals, automatically emailed, or forwarded for review and sign-off for audit/sign-off purposes.

Customer Requirements

Customer agrees to perform the obligations and acknowledges and agrees that Dell SecureWorks' ability to perform its obligations hereunder including the SLAs below are interdependent on Customer's compliance with the following:

Monitored Device Health

Customer is responsible for appropriately maintaining the Devices being monitored and any intermediate systems that convey monitoring data. In the event of a Device failure or misconfiguration, Customer will be responsible for the actions necessary to bring the Device back online. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Portal. SLAs will not apply to devices that are experiencing health issues.

Connectivity

Customer will provide access to Customer-premises and relevant system(s) and management console(s) necessary for Dell SecureWorks to monitor the contracted infrastructure. Additionally, Customer should communicate any network or system changes that could impact Service delivery to the SOC via a ticket in the Portal. SLAs (as defined below) will not apply to Devices that are experiencing Customer-caused connectivity issues.

Service Agreements Level (SLAs)

Service Level Agreements Matrix

SLA	Definition	SLA Credit
Standard Help Desk Requests	Standard help desk requests (applies to all non-change and non-incident tickets) submitted via the Portal or via telephone will be subject to "acknowledgement" (either through the help desk ticketing system, email or telephonically) within one (1) hour from the time stamp on the Help Desk ticket created by Dell SecureWorks.	1/30 th of monthly fee for Service
Security Monitoring	<p>Customer shall receive a response (according to the escalation procedures defined in the Portal or in the manner pre-selected in writing by Customer, either through the Portal, email, or by telephone) to security incidents within fifteen (15) minutes of the determination by Dell SecureWorks that given activity constitutes a security incident. This is measured by the difference between the time stamp on the incident ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation.</p> <p>A "security incident" is defined as an incident ticket that comprises an event (log) or group of events (logs) that is deemed high severity by the SOC in accordance with Dell SecureWorks' Event Handling Process (see Exhibit A). The most up-to-date version can always be found in the Real-Time Events section of the Portal.</p> <p>Automatically created incident tickets (via correlation technology) and event(s) or log(s) deemed low severity will not be escalated, but will be available for reporting through the Portal.</p>	1/30 th of monthly fee for Service for the affected device

Additional Service Rules, Regulations, and Conditions

- a. The Service provides robust security monitoring to Customer. However, deployment of the Service in Customer's network does not eliminate risk, and therefore Dell SecureWorks makes no guarantee that intrusions, compromises, or any other unauthorized activity will not occur on Customer's network.
- b. Dell SecureWorks may schedule maintenance outages for Dell SecureWorks-owned equipment/servers which are being utilized to perform the Services with 24-hours' notice to designated Customer contacts.
- c. The SLAs set forth herein are subject to the following terms, conditions, and limitations:
 - i. The SLAs shall not apply during scheduled maintenance outages, and therefore are not eligible for any SLA credit during these periods. In addition, Dell SecureWorks shall not be held liable for any Service impact related to product configurations that are not supported by Dell SecureWorks within Customer's policy.
 - ii. The SLAs shall not apply in the event of any Customer-caused Service outage that prohibits or otherwise limits Dell SecureWorks from providing the Service, delivering the SLAs, including, but not limited to, Customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software Devices by Customer, its employees, agents, or third parties acting on behalf of Customer.

- iii. Furthermore, the SLAs shall not apply to the extent Customer does not fulfill and comply with the obligations and conditions set forth within this Service Description. The obligations of Dell SecureWorks to comply with the SLAs with respect to any incident response or ticket request are also dependent on Dell SecureWorks' ability to connect directly to Customer Devices on Customer's network through an authenticated server in the SOC.
- d. Dell SecureWorks will troubleshoot and, if necessary, replace any iDevices in accordance with Exhibit B, "Dell SecureWorks Maintenance Program Terms and Conditions."
- e. Customer will receive credit for any failure by Dell SecureWorks to meet the SLAs outlined above within thirty (30) days of notification by Customer to Dell SecureWorks of such SLA failure. In order for Customer to receive an SLA credit, the notification of the SLA failure must be submitted to Dell SecureWorks within thirty (30) days of such SLA failure occurring. Dell SecureWorks will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to Customer in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the MSA, the foregoing SLA credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing SLAs.

Exhibit A – Dell SecureWorks' Event Handling Process

Event Handling Process

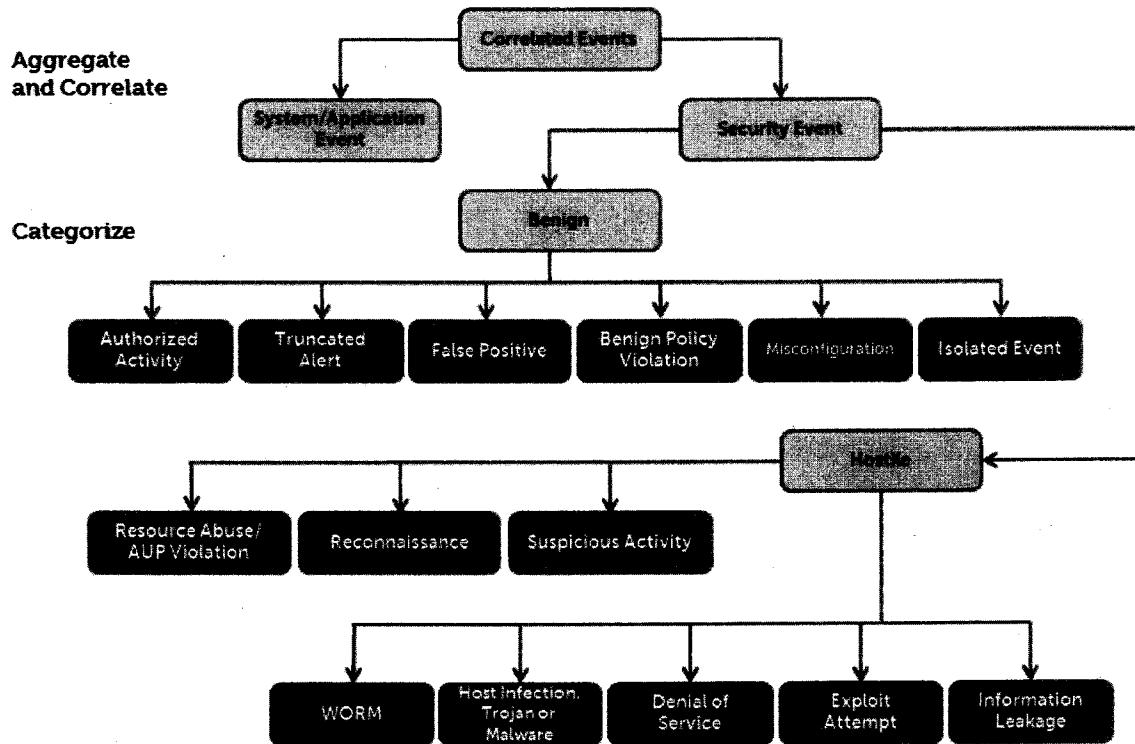


Exhibit B – Dell SecureWorks Maintenance Program ("Program") Terms and Conditions

- Dell SecureWorks agrees, subject to the terms and conditions of the MSA and as further set forth below, to replace Dell SecureWorks iDevices that are not properly functioning adequately due to ordinary wear and tear, malfunctions, or failure. Replacement devices may be new or refurbished. Customer is responsible for purchase of a new device upon End of Life of current device model. Refer to the Dell SecureWorks' Lifecycle Policy for details regarding lifecycle policy, dates and Customer responsibilities.
- iDevices subject to this Program may include the Dell SecureWorks' CTA, iSensor, LogVault appliance, Inspector, SDA, SYSLOG Aggregator, log collection devices, and/or SNORT IDS device.
- If Customer is purchasing an iDevice, the following terms apply:
 1. Mere purchase by Customer of an iDevice does not subject the same to this Program unless:
 - (a) such iDevice is expressly specified in a written Dell SecureWorks Service Order or Service Agreement signed by an authorized officer of Dell SecureWorks and (b) Customer's payment of all maintenance fees is made when due.
 2. Customer may elect to participate in the Program only at the time of purchase of the Dell SecureWorks iDevice. If, at any time after the purchase of the Dell SecureWorks iDevice, Customer wishes to participate in this Program, it must agree to pay all fees that would have been billed since the actual date of purchase of the iDevice.
- The charges for the Program only cover replacement of Dell SecureWorks iDevices. Any performance, damage, repair and/or other warranty issues, or claims with respect to non-Dell SecureWorks-branded iDevices must be addressed with the applicable OEM manufacturer.
- Dell SecureWorks' obligation to comply with the foregoing is conditioned upon, and subject to, the assistance and availability of Customer's onsite personnel for assistance in the: (x) diagnosis and troubleshooting of problems with existing iDevices and (y) replacement and installation of any new iDevice all in compliance with your master service agreement or services schedule.
- Furthermore, Dell SecureWorks will not replace Dell SecureWorks iDevices returned by Customer that are no longer performing on account of unauthorized use, physical damage, or misuse or abuse of the products, as determined by Dell SecureWorks in its sole discretion, including, but not limited to, any of the following circumstances:
 1. Damage due to lightning or other climate problems (including, but not limited to, exposure to excessive light, heat, flooding, and the like).
 2. Opening of iDevices by any person other Dell SecureWorks authorized personnel.
 3. Unauthorized loading or modification of software on or other reprogramming of the iDevice.
 4. Unauthorized linking of the iDevice with other Customer equipment or systems.
 5. Cracks in iDevices, dents to chassis or apparatus, or other damage caused by dropping of iDevice or other mishandling, misuse, or abuse.
 6. Presence of liquids (or residue there from) or the excessive presence of other extraneous materials inside the iDevice (including, but not limited to, dust, hair, dirt, or grime).
 7. Inability to mount the iDevice.
 8. Improper powering down of the iDevice.
- Dell SecureWorks shall bill Customer, and Customer shall be liable, for iDevices: (i) damaged due to misuse or abuse, or (ii) no longer performing adequately due to unauthorized use, physical damage, misuse, or abuse of the iDevices.
- Dell SecureWorks aims to replace iDevices should they fail in the field and the customer has an active maintenance contract in place. In some countries, import process of the foreign country

may impact exchange times. Dell SecureWorks offers spares at a reduced selling price. Customers planning to deploy equipment in countries where import processes can be lengthy are strongly encouraged to purchase spare equipment to maintain.

Exhibit C – Terms and Conditions for Splunk Integration

The following additional terms and conditions apply to the Service when the optional Splunk agent (the "Agent") is deployed to collect monitoring data from a Customer-managed Splunk Enterprise ("Splunk") system:

1. Customer must have an active Splunk Enterprise software license and support contract. The Service cannot be used with free or unlicensed instances of Splunk Enterprise. Dell SecureWorks will specify which versions of the Splunk Enterprise software are supported.
2. Customer is responsible for installation, configuration, and ongoing maintenance of the Splunk software itself as well as administration and maintenance of the hardware platform and/or the virtualization environment the Splunk software runs on.
3. Customer will configure the Splunk software in accordance with minimum required configuration guidelines provided by Dell SecureWorks in order to establish and maintain interoperability.
4. SLAs will not apply in the event that customer is running an unsupported version of the Splunk Enterprise software.
5. Customer must create and maintain a Splunk user account with appropriate privileges for use by the Agent. Configuration guidelines describing this account will be provided during Service Activation. Customer must provide device information during Service Activation as described in the configuration guidelines.
6. SLAs will not apply in the event that Customer's Splunk system is unreachable by the Agent due to network connectivity issues, authentication issues, Splunk configuration issues, or Splunk downtime.
7. Customer is responsible for providing adequate Splunk search resources to handle the Agent's search queries. Dell SecureWorks will provide sizing recommendations. Customer is responsible for evaluating the combined impact of the Agent's activity and other Splunk users and applications to deliver appropriate Splunk search capacity for the agent.
8. In some cases, issue resolution may require discussion of Customer's Splunk environment between Splunk representatives and Dell SecureWorks representatives. Customer must authorize Splunk to participate in such discussions if necessary.
9. Splunk sizing guidelines provided by Dell SecureWorks are estimates and Customer will be responsible for adding resources (RAM, CPU, Additional servers) or reducing log volume in order to improve system performance if Dell SecureWorks determines that this is necessary. Service SLAs will not apply if Customer's Splunk configuration is determined to be inadequate to send the data to Dell SecureWorks..
10. Dell SecureWorks makes no representations as to the compatibility of the Agent with Splunk Applications developed by Splunk or third parties.

Exhibit D – Terms and Conditions for Amazon Web Services Deployment

The following additional terms and conditions apply to the Service when the Virtual Counter Threat Appliance for Amazon Web Services (the "vCTA") is deployed to collect monitoring data from a Customer's Amazon Web Services ("AWS") infrastructure:

1. During all three phases of Service Activation, Customer will be required to provide information about their AWS infrastructure and may be required to make modifications to AWS configuration as specified in the Dell SecureWorks deployment instructions for AWS.
2. Customer must assign and maintain appropriate privileges within their AWS infrastructure to Dell SecureWorks credentials for use by Dell SecureWorks as a part of delivering the Service. Configuration guidelines describing accounts and privileges will be provided during Service Activation.
3. Customer will configure the AWS infrastructure in accordance with required configuration guidelines provided by Dell SecureWorks in order to establish and maintain serviceability.
4. Customer is responsible for all AWS charges incurred within their AWS infrastructure while consuming the Service. These may include but are not limited to: Amazon Elastic Compute Cloud (EC2) instance charges, bandwidth charges, Application Program Interface (API) request charges, and storage charges. It is recommended that the Customer consult AWS pricing pages to estimate costs and to consider cost-reducing strategies such as utilizing reserved EC2 instances.
5. SLAs will not apply in the event that Customer's AWS infrastructure is unreachable due to Customer's network connectivity issues, authentication issues, configuration issues, or AWS downtime.
6. During Service Activation, Dell SecureWorks will provide sizing recommendations and sample deployment scripts, and will describe supported AWS EC2 instance types for iDevices. SLAs will not apply if the Customer chooses an unsupported instance type for their virtual iDevice.
7. In some cases, issue resolution may require discussion of Customer's AWS environment between AWS representatives and Dell SecureWorks representatives. Customer must authorize AWS to participate in such discussions if necessary.

The following terms and conditions apply to the Service when the Service is used to monitor groups of virtual servers ("Elastic Server Groups" or "ESGs") running in Amazon Web Services ("AWS"):

1. Monitoring for Elastic Server Groups is purchased with a fixed upper limit on the number of virtual servers per group (using "up to n " descriptions, where n represents the maximum expected number of EC2 instances in the group), with bursting exceptions as described below. Dell SecureWorks will monitor as few as one server instance per group, regardless of the maximum size.
2. Bursting: The ability to handle dynamic workloads is one of the hallmarks of cloud computing, and so the Dell SecureWorks AWS monitoring service is designed to accommodate occasional spikes, or bursts, of high utilization. ESG monitoring will therefore allow group sizes to exceed their listed limits for brief periods without affecting the delivery of the Service or any SLAs, with the following caveats:
 - a. For group sizes of less than 200, bursts of up to 200% of the listed size will be accommodated (a group of up to 100 servers may burst to 200 servers).

- b. For group sizes between 200 and 1000, bursts of up to 150% of the listed size will be accommodated (a group of up to 250 servers may burst to 325 servers).
 - c. For group sizes greater than 1000, bursts of up to 125% of the listed size will be accommodated (a group of up to 3000 servers may burst to 3750 servers).
 - d. SLAs will not apply in the event that group membership bursts above the levels indicated above.
- 3. Auditing: Dell SecureWorks may audit the Customer's AWS infrastructure to ensure proper licensing of group sizes and numbers of groups to be monitored.
- 4. Group Membership: During Service Activation, Dell SecureWorks will provide information about how the Customer must identify group membership of AWS instances for the purposes of ESG monitoring.

Exhibit 9

Dell SecureWorks Software License and Services Agreements

Attachment 8: Ascent Innovations (Subcontractor) – SecureWorks Service Level Agreements

Ascent Innovations – SecureWorks SLA

Service Level Agreements

Service Level Matrix

SLA	Definition	SLA Credit
Availability	<p>Dell SecureWorks aims for high availability for the Service. This means high availability of the Portal to our customers subscribing to this Service as well as high availability of communications flow between our infrastructure and our customers monitored and managed environments.</p> <p>To attain this goal, Dell SecureWorks maintains communications availability to the Internet 99.9% of the time during any calendar month, excluding planned maintenance windows.</p> <p>"Communications availability" is defined as the ability for one of Dell SecureWorks' SOC's to transmit and receive TCP/IP packets between its networks and its upstream Internet Service Provider.</p> <p>In the event that this SLA is not met for a given calendar month, Customer shall be entitled to a monetary credit equal to 1/30th of the monthly rate paid for the Service(s) delivered during that calendar month. Dell SecureWorks makes no guarantee to availability or performance of the internet at large between Dell SecureWorks' customers to the internet. Dell SecureWorks' measuring of 99.9% is executed from multiple sites throughout the internet to the Dell SecureWorks SOC's.</p>	1/30 th of monthly fee of affected Service
Standard Change Request	<p>Change Requests identified as "Standard" will receive the following Service Levels:</p> <ul style="list-style-type: none"> Acknowledgement of change within one (1) business hour from the time stamp on the help desk ticket created by Dell SecureWorks Scheduling of the change window within six (6) hours of receipt of requirements from Customer Deployment of the change within four (4) hours of the scheduled change window 	1/30 th of monthly fee for Service for the affected Managed Device

All Other help desk Requests	<p>Standard help desk requests (applies to all non-change and non-incident tickets) submitted through the Dell SecureWorks Portal or by telephone will be subject to "acknowledgement" (either through the help desk ticketing system, email, or by telephone) of receiving the request within one (1) hour from the time stamp on the help desk ticket created by Dell SecureWorks.</p> <p>An acknowledgement to help desk requests classified as "Urgent" on the help desk ticket and verified by the SOC as "Urgent" will be sent (either through the help desk ticketing system, email or telephonically) within fifteen (15) minutes from the time stamp on the help desk ticket created by Dell SecureWorks.</p>	1/30 th of monthly fee for Service
Active Health Monitoring	<p>Active health checks identifying the following conditions are subject to the coinciding SLAs below:</p> <ul style="list-style-type: none"> • Device Unreachable – 30 minute response (via phone, ticket or email) from identification of the device being unreachable. This is measured by the difference between the time stamp on the device unreachable ticket created by Dell SecureWorks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation. 	1/30 th of monthly fee for Service for the affected device

1550-14939

EXHIBIT 10

Grant Agreement



Illinois Emergency Management Agency

Jonathon E. Monken, Director

NOTICE OF GRANT AGREEMENT

PART I - Notice of Grant Award to Cook County, Department of Homeland Security and Emergency Management

This Grant Agreement is made and entered into by and between the Illinois Emergency Management Agency (Grantor), 2200 South Dirksen Parkway, Springfield, Illinois 62703, and **Cook County, Department of Homeland Security and Emergency Management (Grantee), Chicago, Illinois 60602-3178.**

The purpose of this Grant is to utilize funds from the Department of Homeland Security (DHS), Federal Fiscal Year 2014 **Homeland Security Grant Program (HSGP), Urban Area Security Initiative (UASI), CFDA #97.067.** UASI funds from the HSGP grant are intended to support homeland security projects directly benefiting Chicago's high-risk Urban Area.

The Grantor hereby grants to the Grantee an amount not exceeding **\$27,650,598.95** for the period from **September 1, 2014, to March 31, 2016.** The Grantee hereby agrees to use the funds provided under the Agreement for the purposes set forth herein and agrees to comply with all terms and conditions of this Agreement and applicable federal and state policies and grant guidance.

The Grantee shall include all requirements listed herein in each subgrant, contract and subcontract financed in whole or in part with federal assistance.

This Agreement and attachments constitute the entire agreement between the parties and there are no oral agreements or understanding between the parties other than what has been reduced to writing herein.

PART II - Term

The term of this Agreement shall be from **September 1, 2014, to March 31, 2016.**

PART III - Scope of Work

The Grantee will utilize the Homeland Security Grant Program (HSGP) funding as outlined in the Grantee's FFY 2014 Grant Program Application. The HSGP funds shall be used for costs related to the planning, organization, equipment, training, and exercise needs that prevent, protect against, mitigate, respond to, and recover from acts of terrorism and other catastrophic events.

The Budget Detail Worksheet in Attachment A outlines a description of the expenditures for which the Grantee will seek reimbursement. The Grantor will only reimburse those activities that are specifically listed in the Budget Detail Worksheet, except as provided in Part VI herein.

The Project Implementation Worksheet in Attachment A provides a detailed description of the scope of work to be performed using funds received through this Agreement, including a list of specific outcomes and sequential milestones that will be accomplished by the Grantee. These milestones will allow the Grantor to measure progress of the Grantee in achieving the goals of the project.

PART IV - Compensation Amount

The total compensation and reimbursement payable by the Grantor to the Grantee shall not exceed the sum of **\$27,650,598.95.**



2200 S. Dirksen Parkway • Springfield, Illinois • 62703 • Telephone (217) 782-7860 • <http://www.iema.illinois.gov>

Printed by the authority of the State of Illinois on Recycled Paper

PART V - Terms and Conditions

SPENDING LIMITATIONS: All allocations and use of funds by the Grantee shall be in accordance with applicable funding opportunity announcements, grant guidance and application kits. The Grantee shall comply with all applicable federal and state statutes, regulations, executive orders, and other policies and requirements in carrying out any project supported by these funds. The Grantee recognizes that laws, regulations, policies, and administrative practices may be modified from time to time and those modifications may affect project implementation. The Grantee agrees that the most recent requirements will apply during the performance period of this Agreement. All subgrants issued by the Grantee to this Agreement in excess of \$25,000.00 must be pre-approved by the Grantor.

FISCAL FUNDING: The Grantor's obligations hereunder shall cease immediately, without penalty or further payment being required, in any year for which the General Assembly of the State of Illinois fails to make an appropriation sufficient to pay such obligation or the U.S. Department of Homeland Security, Federal Emergency Management Agency, Grants Programs Directorate (DHS FEMA GPD) fails to provide the funds. The Grantor shall give the Grantee notice of such termination for funding as soon as practicable after the Grantor becomes aware of the failure of funding. The Grantee's performance obligations under the Agreement shall cease upon notice by the Grantor of lack of appropriated funds.

METHOD OF COMPENSATION: The Grantee must submit vendor invoices or a computer generated report with description of costs, including a statement of payment for personnel costs and affirmation or evidence of delivery and property identification numbers for property subject to the Grantor's policies and procedures, in order to receive compensation through this Agreement. Such invoices and reports must be submitted to the Grantor in a timely manner, and in no event later than 30 days following the expiration of this Agreement. The method of compensation shall be reimbursement in accordance with the invoice voucher procedures of the Office of the State of Illinois Comptroller. The Grantor will not reimburse the Grantee for any exercise expenditures unless and until an After Action Report/Improvement Plan is submitted in accordance with "Part V—Reports" herein. The Grantee shall maintain appropriate records of actual costs incurred and submit expenditure information to the Grantor. The Grantee shall comply with the requirements of 31 U.S.C. 3729, which provides that no recipient of federal payments shall submit a false claim for payment. No costs eligible under this Agreement shall be incurred after **March 31, 2016**.

NON-SUPPLANTING REQUIREMENT: The Grantee agrees that funds received under this award will be used to supplement, but not supplant, state or local funds for the same purposes. The Grantee may be required to demonstrate and document that a reduction in non-federal resources occurred for reasons other than the receipt or expected receipt of federal funds.

REPORTS: The Grantee shall provide a quarterly update of the Project Implementation Worksheet in Attachment A to the Grantor within fifteen (15) business days after March 31, June 30, September 30, and December 31 throughout the performance period of the Agreement. Upon written request, the Grantee shall submit to the Grantor, within 15 days after the end of the reporting period (July 15 for the reporting period of January 1 through June 30 and January 15 for the reporting period of July 1 through December 31) throughout the stated performance period, the following documentation: Discipline Allocation Report and Grant-Funded Typed Resource Report. If the Grantee has no typed resources to report within the Grant-Funded Typed Resource Report, the Grantee must notify the Grantor in writing of that fact, upon written request. The Grantee must, upon written request, submit a final Budget Detail Worksheet, Discipline Allocation Worksheet, Project Implementation Worksheet and Grant-Funded Typed Resource Report to the Grantor within 30 days after the expiration of the Agreement.

The Grantee also must submit a final After Action Report/Improvement Plan to the Grantor within 45 days after each exercise. All exercises conducted with funds provided through this Agreement must be National Incident Management System (NIMS) compliant and be managed and executed in accordance with the Homeland Security Exercise and Evaluation Program (HSEEP).

ACCOUNTING REQUIREMENTS: The Grantee shall maintain effective control and accountability over all funds, equipment, property, and other assets under this Agreement. The Grantee shall keep records sufficient to permit the tracing of funds to ensure that expenditures are made in accordance with this Agreement. The Grantee must follow the retention and access requirements for records [44 CFR 13.42 (b) and 2 CFR 215.531]. All records must be maintained for three years after submission of the final expenditure report; or if any litigation, claim or audit is started before the expiration of the three-year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken. The Grantee shall assure subgrants are in compliance with 44 CFR 13.37. Funds received by the Grantee must be placed in an interest-bearing account.

The Grantee shall comply with the most recent version of the Administrative Requirements and Cost Principles, as applicable. A non-exclusive list of regulations commonly applicable to the DHS FEMA GPD grants are listed below:

- A. Administrative Requirements
 - 1. 44 CFR Part 13, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments (OMB Circular A-102)
 - 2. 2 CFR Part 215, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations (OMB Circular A-110)
- B. Cost Principles
 - 1. 2 CFR Part 225, Cost Principles for State, Local and Indian Tribal Governments (OMB Circular A-87)
 - 2. 2 CFR Part 220, Cost Principles for Educational Institutions (OMB Circular A-21)
 - 3. 2 CFR Part 230, Cost Principles for Non-Profit Organizations (OMB Circular A-122)
 - 4. Federal Acquisition Regulations (FAR), Part 31.2 Contract Cost Principles and Procedures, Contracts with Commercial Organizations

DUPLICATION OF BENEFITS: The Grantee shall not duplicate any federal assistance, per 2 CFR Part 225, Basic Guidelines Section C.3 (c), which provides that any cost allocable to a particular federal award or cost objective under the principles provided for in this Authority may not be charged to other federal awards to overcome fund deficiencies, to avoid restrictions imposed by law or terms of the federal awards, or for other reasons. However, this prohibition does not preclude the Grantee from shifting costs that are allowable under two or more awards in accordance with existing program agreements. Non-governmental entities are subject to this prohibition per 2 CFR Parts 220 and 230 and FAR Part 31.2.

RECORD KEEPING AND AUDITS: Grantee shall maintain records for equipment, non-expendable personal property, and real property. The Grantee shall, as often as deemed necessary by the Grantor, DHS FEMA GPD or any of their duly authorized representatives, permit the Grantor, DHS FEMA GPD, the Auditor General, the Attorney General or any of their duly authorized representatives to have full access to and the right to examine any pertinent books, documents, papers and records of the Grantee involving transactions related to this Agreement. The Grantee shall cooperate with any compliance review or complaint investigation conducted by DHS. The Grantee shall submit timely, complete and accurate reports and claims for payment and shall maintain appropriate backup documentation. The Grantee shall comply with all other special reporting, data collection and evaluation requirements as may be required by DHS. The Grantee acknowledges that these are federal pass-through funds that must be accounted for in the jurisdiction's Single Audit under the Single Audit Act of 1996, if required. The Grantee certifies that all audits submitted under the provisions of OMB Circulars A-133, Audits of States, Local Governments, and Non-Profit Organizations, have been approved by the Grantor.

MODIFICATION AND AMENDMENT OF THE GRANT: This Agreement is subject to revision as follows:

- A. Modifications may be required because of changes in state or federal laws, regulations, or federal grant guidance as determined by the Grantor. Any such required modification shall be incorporated into and will be part of this Agreement. The Grantor shall notify the Grantee of any pending implementation of or proposed amendment to such regulations before a modification is made to the Agreement.
- B. Modifications may be made upon written agreement of both the Grantor and Grantee.

TERMINATION FOR CONVENIENCE: This Agreement may be terminated in whole or in part by the Grantor for its convenience, provided that, prior to termination, the Grantee is given: 1) not less than ten (10) calendar days written notice by certified mail, return receipt requested, of the Grantor's intent to terminate, and 2) an opportunity for consultation with the Grantor prior to termination. In the event of partial or complete termination of this Agreement pursuant to this paragraph, an equitable adjustment of costs shall be paid to the Grantee for expenses incurred under this Agreement prior to termination.

TERMINATION FOR BREACH OR OTHER CAUSE: The Grantor may terminate this Agreement without penalty to the Grantor or further payment required in the event of:

- A. Any breach of this Agreement that, if it is susceptible of being cured, is not cured within 15 calendar days after receipt of the Grantor's notice of breach to the Grantee.

- B. Material misrepresentation or falsification of any information provided by the Grantee in the course of any dealing between the parties or between the Grantee and any state agency.

The Grantee's failure to comply with any one of the terms of this Agreement shall be cause for the Grantor to seek recovery of all or part of the grant proceeds.

SEVERABILITY CLAUSE: If any provision under this Agreement or its application to any person or circumstance is held invalid by any court of competent jurisdiction, this invalidity does not affect any other provision or its application of this Agreement which can be given effect without the invalid provision or application.

WORKER'S COMPENSATION INSURANCE, SOCIAL SECURITY, RETIREMENT AND HEALTH INSURANCE BENEFITS, AND TAXES: The Grantee shall provide worker's compensation insurance where the same is required, and shall accept full responsibility for the payment of unemployment insurance, premiums for worker's compensation, social security and retirement and health insurance benefits, as well as all income tax deductions and any other taxes or payroll deductions required by law for employees of the Grantee who are performing services specified by this Agreement.

WAIVERS: No waiver of any condition of this Agreement may be effective unless in writing from the Director of the Grantor.

WORK PRODUCT: The Grantee acknowledges DHS FEMA GPD and State of Illinois reserve a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and authorize others to use, for federal and state purposes: (1) the copyright in any work developed under an award or subaward; and (2) any rights of copyright to which a recipient or subrecipient purchases ownership with federal support. The Grantee agrees to consult with DHS FEMA GPD, through the Grantor, regarding the allocation of any patent rights that arise from, or are purchased with, this funding. All publications created through this Agreement shall affix the applicable copyright notices of 17 U.S.C. 401-402 and prominently contain the following statement: *"This document was prepared under a grant from the Federal Emergency Management Agency's Grant Program Directorate (FEMA/GPD) within the U.S. Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of FEMA/GPD, the U.S. Department of Homeland Security or the State of Illinois."*

ACKNOWLEDGEMENT OF FEDERAL FUNDING: The Grantee shall acknowledge federal funding when issuing statements, press releases, requests for proposals, bid invitations, and other documents describing projects or programs funded in whole or in part with federal funds.

RECAPTURE OF FUNDS: The Grantee shall return to the Grantor all state or federal grant funds that are not expended or received from the Grantor in error. All funds remaining at the expiration of the period of time the funds are available for expenditure or obligation by the Grantee shall be returned to the Grantor within 45 days, if applicable. The Grantor may recapture those funds in accordance with state and federal laws and regulations. The Grantee's failure to comply with any one of the terms of this Agreement shall be cause for the Grantor to seek recovery of all or part of the grant proceeds.

MAINTENANCE AND REVIEW OF EQUIPMENT: The Grantor reserves the right to reclaim or otherwise invoke the Illinois Grant Funds Recovery Act on any and all equipment purchased by the Grantee with grant funds if said equipment is not properly maintained or has fallen into neglect or misuse according to the standards and policies of the Grantor. Additionally, the Grantee may not substitute, exchange or sell any equipment purchased with grant funds unless the Grantee has the express written consent of the Grantor. All equipment procured by the Grantee through this Agreement shall be made available for review by the Grantor upon request. The Grantee agrees that, when practicable, any equipment purchased with grant funding shall be prominently marked as follows: *"Purchased with funds provided by the U.S. Department of Homeland Security."*

POSSESSION OF EQUIPMENT: Title to equipment acquired by a non-federal entity with federal awards vests with the Grantee. Equipment means tangible nonexpendable property, including exempt property, charged directly to the award having a useful life of more than one year and an acquisition cost of \$5,000 or more per unit. However, consistent with a non-federal entity's policy, lower limits may be established. The Grantee shall use, manage, and dispose of equipment acquired under a federal grant in accordance with federal and state laws, procedures and policies. All equipment purchased with funding received through this Agreement shall be used, for the entire useful life of the equipment, in accordance with the purpose stated in PART III – Scope of Work. Any variation to the intended use of the equipment outlined in PART III – Scope of Work by the Grantee must be approved in writing by the Grantor.

SAFECOM: If funding will be used to purchase emergency communications equipment or fund related activities, the Grantee shall comply with the SAFECOM Guidance for Emergency Communication Grants, including provisions on technical standards that ensure and enhance interoperable communications.

LIABILITY: The Grantor assumes no liability for actions of the Grantee under this Agreement, including, but not limited to, the negligent acts and omissions of Grantee's agents, employees, and subcontractors in their performance of the Grantee's duties as described under this Agreement. In addition, the Grantor makes no representations, or warranties, expressed or implied, as to fitness for use, condition of, or suitability of said equipment purchased pursuant to this Agreement, except as those representations are made by the manufacturer of said equipment. As to nature and condition of said equipment, in the use of said equipment, the Grantee agrees to hold the Grantor harmless for any defects or misapplications. To the extent allowed by law, the Grantee agrees to hold harmless the Grantor against any and all liability, loss, damage, cost or expenses, including attorney's fees, arising from the intentional torts, negligence, or breach of the Agreement by the Grantee, with the exception of acts performed in conformance with an explicit, written directive of the Grantor.

ENVIRONMENTAL AND HISTORIC PRESERVATION (EHP) COMPLIANCE: The Grantee shall not undertake any project having the potential to impact Environmental or Historical Preservation (EHP) resources without the prior approval of DHS FEMA GPD, including but not limited to communications towers, physical security enhancements, new construction, and modifications to buildings, structures and objects that are 50 years old or greater. The Grantee must comply with all conditions placed on the project as the result of the EHP review. Any change to the approved project scope of work will require re-evaluation for compliance with these EHP requirements. If ground disturbing activities occur during project implementation, the Grantee must ensure monitoring of ground disturbance, and if any potential archeological resources are discovered, the Grantee will immediately cease construction in that area and notify DHS FEMA GPD and the appropriate State Historic Preservation Office. Any construction activities that have been initiated without the necessary EHP review and approval will result in the non-compliance finding and will not be eligible for DHS FEMA GPD funding.

AMERICANS WITH DISABILITIES ACT (ADA): The Grantee understands the importance of integrating disability access and functional needs efforts into local homeland security and emergency preparedness programs. This integration should occur at all levels from planning, to purchasing equipment and supplies, to conducting exercises and drills and should involve disability inclusion experts as partners across all aspects of emergency planning.

FEIN: Under penalties of perjury, the Grantee certifies that **36-6006541** is its correct Federal Taxpayer Identification Number and that IRS Instructions have been provided for proper completion of this certification. The Grantee files with the IRS as a (please check one):

<input type="checkbox"/> Individual	<input type="checkbox"/> Real Estate Agent
<input type="checkbox"/> Sole Proprietorship	<input checked="" type="checkbox"/> Governmental Entity
<input type="checkbox"/> Partnership	<input type="checkbox"/> Tax Exempt Organization (IRC 501(a) only)
<input type="checkbox"/> Corporation	<input type="checkbox"/> Trust or Estate
<input type="checkbox"/> Medical and Health Care	<input type="checkbox"/> Services Provider Corporation

CERTIFICATION: The Grantee certifies under oath that all information in the Agreement is true and correct to the best of the Grantee's knowledge, information, and belief; that the funds shall be used only for the purposes described in the Agreement; and that the award of grant funds is conditioned upon such certification.

PART VI – Special Conditions

Each of the following conditions applies to this Agreement. The failure of the Grantee to fulfill one or more condition will result in the Grantor holding reimbursement of funds until all such noncompliant conditions are met.

1. The Grantee must allocate 25 percent of funds towards law enforcement terrorism prevention activities.
2. The Grantee shall provide to the Grantor by December 15, 2014, an update to the Urban Area Threat and Hazard Identification and Risk Assessment that aligns with the CPG 201, Second Edition, and is inclusive of all jurisdictions within the Urban Area.

2014 Grant Agreement

2014 Federal Fiscal Grant Year – Cook County, Department of Homeland Security and Emergency Management

14UASICOOK

Page 5 of 10

3. The Grantee shall provide to the Grantor within 30 days of the final execution of this Agreement the name and contact information for the specific point of contact for coordinating the following grant-related activities: (1) scheduling and conduct of quarterly Urban Area Working Group (UAWG) meetings, (2) management and administration of this Agreement, (3) property control and sub-recipient monitoring, (4) training and education, (5) exercises, and (6) Environmental and Historic Preservation submissions.
4. The Grantee shall submit to the Grantor by December 31, 2015, an Urban Area multi-year training and exercise plan that aligns with the Urban Area Homeland Security Strategy.
5. The Grantee shall submit to the Grantor within 30 days of the final execution of this Agreement a membership roster for the UAWG. The membership must directly or indirectly represent all relevant jurisdictions and response disciplines (including law enforcement, fire service, EMS, and emergency management) that comprise the defined Urban Area and include local Citizen Corps Council or their equivalent.
6. The Grantee shall ensure that the Urban Area conducts at minimum one quarterly meeting of the UAWG within the periods of October 1, 2014, to December 31, 2014, January 1, 2015, to March 31, 2015, April 1, 2015, to June 30, 2015, July 1, 2015, to September 30, 2015, October 1, 2015, to December 31, 2015, and January 1, 2016, to March 31, 2016. At a minimum, the UAWG shall provide at each meeting an update on the development and implementation of all program initiatives funded through this Agreement. The Grantee must provide to the Grantor within 30 days of the final execution of this Agreement an UAWG meeting schedule that comports with the meeting requirements listed herein. The failure of the Urban Area to conduct a meeting during a quarter will result in the Grantor suspending reimbursement of the Grantee's funds until a meeting is conducted.

PART VII– Other Requirements

PERSONALLY IDENTIFIABLE INFORMATION (PII): If the Grantee collects PII, the Grantee is required to have a publicly available privacy policy that describes what PII it collects, how it uses PII, whether it shares PII with third parties, and how individuals may have their PII corrected where appropriate.

CONFLICT OF INTEREST: No official or employee of the Grantee who is authorized in the Grantee's official capacity to negotiate, make, accept, or approve, or to take part in such decisions regarding a contract for acquisition/development of property in connection with this Agreement, shall have any financial or other personal interest in any such contract for the acquisition/development. No federal employees shall receive any funds under this award. Federal employees are prohibited from serving in any capacity (paid or unpaid) on any proposal submitted under this program. The Grantee certifies that it will establish safeguards to prohibit employees, contractors, and subcontractors from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

HATCH ACT: The Grantee will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328), which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds.

ACTIVITIES CONDUCTED ABROAD: The Grantee shall comply with the requirements that project activities carried on outside the United States are coordinated as necessary with appropriate government authorities and that appropriate licenses, permits, or approvals are obtained.

USE OF FUNDS: The Grantee shall not use any federal funds, either directly or indirectly, in support of the enactment, repeal, modification or adoption of any law, regulation or policy, at any level of government, without the express prior written approval of the Grantor.

USE OF SEAL, LOGO AND FLAGS: The Grantee must obtain DHS's approval prior to using a DHS or United States Coast Guard seal, logo, crest or reproduction of flags or likenesses of DHS agency or Coast Guard officials.

DELINQUENCY: The Grantee shall not be delinquent in the repayment of any federal debt, including but not limited to delinquent payroll or other taxes, audit disallowances, and benefit overpayments.

2014 Grant Agreement

2014 Federal Fiscal Grant Year – Cook County, Department of Homeland Security and Emergency Management

14UASICOOK

Page 6 of 10

PUBLIC WORKS PROJECTS: Any public works project supported with funds received through this Agreement must employ at least 90 percent Illinois' laborers on such project during periods of excessive unemployment in Illinois. "Public works" is defined as any fixed work construction or improvement for the State of Illinois, or any political subdivision of the State funded or financed in whole or in part with state funds or funds administered by the State of Illinois. "Period of excessive unemployment" is defined as any month immediately following two consecutive calendar months during which the level of unemployment in the State of Illinois has exceeded five percent.

NON-DISCRIMINATION: In carrying out the program, the Grantee will comply with all applicable federal laws relating to nondiscrimination including, but not limited to:

- Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d, which prohibits discrimination on the basis of race, color, or national origin;
- Title IX of the Education Amendments of 1972, as amended, 20 U.S.C. 1681 through 1683, and 1685 through 1687, and U.S. DOT regulations, "Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance", 49 CFR Part 25, which prohibit discrimination on the basis of sex;
- Section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. 794, which prohibits discrimination on the basis of handicap;
- The Age Discrimination Act of 1975, as amended 42 U.S.C. 6101 through 6107, which prohibits discrimination on the basis of age;
- The Drug Abuse Office and Treatment Act of 1972, Pub. L. 92-255, March 21, 1972, and amendments thereto, 21 U.S.C. 1174 *et seq.* relating to nondiscrimination on the basis of drug abuse;
- The Comprehensive Alcohol Abuse and Alcoholism Prevention Act of 1970, Pub. L. 91-616, Dec. 31, 1970, and amendments thereto, 42 U.S.C. 4581 *et seq.* relating to nondiscrimination on the basis of alcohol abuse or alcoholism;
- The Public Health Service Act of 1912, as amended, 42 U.S.C. 290dd-3 and 290ee-3, related to confidentiality of alcohol and drug abuse patient records;
- Title VIII of the Civil Rights Act of 1968, 42 U.S.C. 3601 *et seq.*, relating to nondiscrimination in the sale, rental, or financing of housing;
- The Americans with Disabilities Act of 1990, as amended and 42 U.S.C. 12101 *et seq.*;
- Any other nondiscrimination provisions in the specific statutes under which federal assistance for the project may be provided; and
- Any other nondiscrimination statute(s) that may apply to the project.

The Grantee shall take affirmative action to ensure that applicants for employment are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, national origin, ancestry, age, physical or mental handicap unrelated to ability, marital status, or unfavorable discharge from military service. Such action shall include, but not be limited to, the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training including apprenticeship. The Grantee shall post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Government setting forth the provisions of this non-discrimination clause.

The Grantee shall disclose all instances in the past three years in which the Grantee has been accused of discrimination on the grounds of race, color, national origin (including limited English proficiency), sex, age, disability, religion, or familial status against the recipient or the recipient settles a case or matter alleging discrimination, including outcomes and settlement agreements.

DEBARMENT: The Grantee shall comply with debarment provisions as contained in Executive Orders 12549 and 12689, as well as 49 CFR Part 29, including Appendices A and B as amended. The Grantee certifies that to the best of its knowledge and belief, Grantee and Grantee's principals: a) are not presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from covered transactions by any federal agency; b) within a three-year period preceding this Agreement have not been convicted of or had a civil judgment rendered against it for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain or performing a public (federal, state or local) transaction or contract under a public transaction, violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records making false statements receiving stolen property; c) are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offences enumerated in subsection (b), above; d) have not within a three-year period preceding this Agreement had one or more public transactions (federal, state, or local) terminated for cause or default.

2014 Grant Agreement

2014 Federal Fiscal Grant Year – Cook County, Department of Homeland Security and Emergency Management

14UASICOOK

Page 7 of 10

The inability of the Grantee to certify to the certification in this section will not necessarily result in denial of participation in the Agreement. The Grantee shall submit an explanation of why it cannot provide the certification in this section. This certification is a material representation of fact upon which reliance was placed when the Grantor determined whether to enter into this transaction. If it is later determined that Grantee knowingly rendered an erroneous certification, in addition to other remedies available to the federal government, the Grantor may terminate this Agreement for cause. The Grantee shall provide immediate written notice to the Grantor if at any time the Grantee learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this section shall have the meaning set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549.

The Grantee agrees that it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible or voluntarily excluded from participation in this covered transaction, unless authorized, in writing, by the Grantor. The Grantee agrees that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion-Lower Tier Covered Transaction" provided by the Grantor, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions. The Grantee may rely upon a certification of a prospective participant in a lower tier covered transaction, unless Grantee knows the certification is erroneous. Grantee may decide the method and frequency by which it determines the eligibility of its principals. The Grantee may, but is not required to, check the Non-procurement List. If a Grantee knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation, in addition to other remedies available to the federal government, the Grantor may terminate this Agreement for cause or default.

LOBBYING: In accordance with 31 U.S.C. 1352, the Grantee certifies to the best of his or her knowledge and belief that:

- A. No federally appropriated funds have been or will be paid by or on behalf of the Grantee to any person to influence or attempt to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress regarding the award of federal assistance or the extension, continuation, renewal, or amendment, of federal assistance, or the extension, continuation, renewal, amendment, or modification of any federal assistance agreement; and
- B. If any funds other than federally appropriated funds have been or will be paid to any person to influence or attempt to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any application for federal assistance, the Grantee assures that it will complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying."

The language of this certification shall be included in the award documents for all subawards at all tiers (including subcontracts, sub grants, and contracts under grants, loans, and cooperative agreements).

BOYCOTT: The Grantee certifies that neither it nor any substantially-owned affiliated company is participating or shall participate in an international boycott in violation of the provisions of the U.S. Export Administration Act of 1979 or the regulations of the U.S. Department of Commerce promulgated under that Act.

NIMS COMPLIANCE: The Grantee certifies that it has fully implemented all current National Incident Management System compliance activities in accordance with Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents* and related compliance documentation provided by the Secretary of Homeland Security and State of Illinois.

ANTI-BRIBERY: The Grantee certifies that it has not been convicted of bribery or attempting to bribe an officer or employee of the State of Illinois, nor has any official, agent, or employee of the Grantee committed bribery or attempted bribery on behalf of the Grantee and pursuant to the direction or authorization of a responsible official of the Grantee.

BIDDING: The Grantee hereby certifies that it has not been barred from bidding on or receiving state or local government contracts as a result of illegal bid rigging or bid rotating as defined in the Criminal Code of 2012 (720 ILCS 5/33E-3 and 33E-4).

OTHER APPLICABLE LAWS: The Grantee certifies that it will comply with all applicable federal laws, regulations, and orders, including the following:

- Trafficking Victims Protection Act of 2000, as amended, 22 U.S.C. 7104 and 2 CFR Part 175;

2014 Grant Agreement

2014 Federal Fiscal Grant Year – Cook County, Department of Homeland Security and Emergency Management

14UASICOOK

Page 8 of 10

- Fly America Act of 1974;
- Executive Order 13166 regarding persons with Limited English Proficiency;
- Animal Welfare Act of 1966, 7 U.S.C. 2131;
- Clean Air Act of 1970 and Clean Water Act of 1977, 42 U.S.C. 7401 and related Executive Order 11738;
- Protection of Human Subjects for research purposes, 45 CFR Part 46;
- National Environmental Policy Act of 1969, as amended, 42 U.S.C. 4331;
- National Flood Insurance Act of 1968, as amended, 42 U.S.C. 4102, and regulations codified at 44 CFR Part 63;
- Flood Disaster Protection Act of 1973, as amended, 42 U.S.C. 4001;
- Coastal Wetlands Planning, Protection, and Restoration Act of 1990 and related Executive Order 11990;
- USA Patriot Act of 2001, 18 U.S.C. 175; and
- Hotel and Motel Fire Safety Act of 1990, 15 U.S.C. 2225, which requires the Grantee to ensure that all conference, meeting, convention, or training space funded in whole or in part with federal funds complies with the fire prevention and control.

WAGES: The Grantee certifies that to the extent applicable, grantee will comply with the Davis-Bacon Act, as amended, 40 U.S.C. 3141 *et seq.*, the Copeland "Anti-Kickback" Act, as amended, 18 U.S.C. 874, and the Contract Work Hours and Safety Standards Act, as amended, 40 U.S.C. 3701 *et seq.*, regarding labor standards for federally assisted sub agreements.

DRUG FREE CERTIFICATION: This certification is required by the federal Drug-Free Workplace Act of 1988 (41 USC 702) and the Illinois Drug Free Workplace Act (30 ILCS 580). No grantee or contractor shall receive a grant or be considered for the purposes of being awarded a contract for the procurement of any property or services from the United States or the State of Illinois unless that grantee or contractor has certified to the United States or the State of Illinois that the grantee or contractor will provide a drug free workplace. False certification or violation of the certification may result in sanctions including, but not limited to, suspension of contract or grant payments, termination of the contractor or grant and debarment of contracting or grant opportunities with the State for at least one (1) year but not more than five (5) years.

For the purpose of this certification, "grantee" or "contractor" means a corporation, partnership, or other entity with twenty-five (25) or more employees at the time of issuing the grant, or a department, division, or other unit thereof, directly responsible for the specific performance under a contract or grant of \$5,000 or more from the State.

The Grantee certifies and agrees that it will provide a drug free workplace by:

- A. Publishing a statement:
 - (1) Notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance, including cannabis, is prohibited in the Grantee's or contractor's workplace.
 - (2) Specifying the actions that will be taken against employees for violations of such prohibition.
 - (3) Notifying the employee that, as a condition of employment on such contract or grant, the employee will:
 - a. Abide by the terms of the statement; and
 - b. Notify the employer of any criminal drug statute conviction for a violation occurring in the workplace no later than five (5) days after such conviction.
- B. Establishing a drug free awareness program to inform employees about:
 - (1) the dangers of drug abuse in the workplace;
 - (2) the Grantee's or contractor's policy of maintaining a drug free workplace;
 - (3) any available drug counseling, rehabilitation, and employee assistance programs; and
 - (4) the penalties that may be imposed upon an employee for drug violations.
- C. Providing a copy of the statement required by subparagraph (a) to each employee engaged in the contract or grant and to post the statement in a prominent place in the workplace.
- D. Notifying the Grantor within ten (10) days after receiving notice under part (B) of paragraph (3) of subsection (a) above from an employee or otherwise receiving actual notice of such conviction.
- E. Imposing a sanction on or requiring the satisfactory participation in a drug abuse assistance or rehabilitation program by any employee who is so convicted, as required by section 5 of the Drug Free Workplace Act.

2014 Grant Agreement

2014 Federal Fiscal Grant Year – Cook County, Department of Homeland Security and Emergency Management

14UASICOOK

Page 9 of 10

- F. Assisting employees in selecting a course of action in the event drug counseling, treatment, and rehabilitation are required and indicating that a trained referral team is in place.
- G. Making a good faith effort to continue to maintain a drug free workplace through implementation of the Drug Free Workplace Act.

IN WITNESS WHEREOF, the parties hereto have caused this contract to be executed by their duly authorized representatives.

Grantor: IL Emergency Management Agency

Grantee: **Cook County, Department of Homeland Security and
Emergency Management**

By: _____
Jonathon E. Monken, Director

By: _____
Michael Masters, Executive Director

DATE: _____

DATE: _____

By: _____
Kevin High, Chief Fiscal Officer

DATE: _____

By: _____
Jenifer Johnson, Chief Legal Counsel

DATE: _____

14UASICOOK

2014 Grant Agreement

2014 Federal Fiscal Grant Year – Cook County, Department of Homeland Security and Emergency Management

14UASICOOK

Page 10 of 10



ILLINOIS EMERGENCY MANAGEMENT AGENCY

Bruce Rauner
Governor

James K. Joseph
Director

ILLINOIS EMERGENCY MANAGEMENT AGENCY GRANT ADJUSTMENT NOTICE 14UASICOOK - GAN #1

Changes/additions are in *italic type*.

Part I – Notice of Grant Award to Cook County, Department of Homeland Security and Emergency Management

This Grant Adjustment Notice (GAN) is made and entered by and between the Illinois Emergency Management Agency (Grantor), 2200 South Dirksen Parkway, Springfield, Illinois 62703-4528, and the Cook County, Department of Homeland Security and Emergency Management (Grantee), 69 West Washington Street, Suite 2600, Chicago, Illinois 60602-3178.

The purpose of this Grant is to utilize funds from the Department of Homeland Security (DHS), Federal Fiscal Year 2014 Homeland Security Grant Program, Urban Area Security Initiative (UASI), CFDA #97.067. ...

The Grantor hereby grants to the Grantee an amount not exceeding \$27,650,598.95 for the period from September 1, 2014, to July 31, 2016. ...

PART II – Term

The term of this Grant Agreement shall be from September 1, 2014, to July 31, 2016.

PART V – Terms and Conditions

METHOD OF COMPENSATION: The Grantee must... No costs eligible under this Agreement shall be incurred after July 31, 2016.

Except as set forth herein, all other terms and conditions of the Agreement remain in full force and effect.

IN WITNESS WHEREOF, the Grantee and Grantor have caused this amendment to be executed on the dates shown below by representatives authorized to bind the respective Parties.

Grantor: IL Emergency Management Agency

Grantee: Cook County, Department of Homeland Security and Emergency Management

Signature: 

James K. Joseph, Director

Signature: 

Ernest Brown, Executive Director

By: 

Lisa M. Desai, Assistant to the Director

Date: 2/4/2016

Date: 2-5-16

14UASICOOK (Extend time period through July 31, 2016)

1550-14939

EXHIBIT 11

Federal Clause

Exhibit 8
Cook County Information Technology Special Conditions (ITSCs)

1. DEFINITIONS FOR SPECIAL CONDITIONS

1.1. **"Assets"** means Equipment, Software, Intellectual Property, IP Materials and other assets used in providing the Services. Assets are considered in use as of the date of deployment.

1.2. **"Business Associate Agreement" or "BAA"** means an agreement that meets the requirements of 45 C.F.R. 164.504(e).

1.3. **"Business Continuity Plan"** means the planned process, and related activities, required to maintain continuity of business operations between the period of time following declaration of a Disaster until such time an IT environment is returned to an acceptable condition of normal business operation.

1.4. **"Cardholder Data"** means data that meets the definition of "Cardholder Data" in the most recent versions of the Payment Card Industry's Data Security Standard.

1.5. **"Change"** means, in an operational context, an addition, modification or deletion to any Equipment, Software, IT environment, IT systems, network, device, infrastructure, circuit, documentation or other items related to Services. Changes may arise reactively in response to Incidents/Problems or externally imposed requirements (e.g., legislative changes), or proactively from attempts to (a) seek greater efficiency or effectiveness in the provision or delivery of Services; (b) reflect business initiatives; or (c) implement programs, projects or Service improvement initiatives.

1.6. **"Change Management"** means, in an operational context, the Using Agency approved processes and procedures necessary to manage Changes with the goal of enabling Using Agency-approved Changes with minimum disruption.

1.7. **"Change Order"** means a document that authorizes a Change to the Services or Deliverables under the Agreement, whether in time frames, costs, or scope.

1.8. **"Change Request"** means one Party's request to the other Party for a Change Order.

1.9. **"Contractor"** has the same meaning as either: (a) both "Contractor" and "Consultant" as such terms are defined, and may be interchangeably used in the County's Professional Services Agreement, if such document forms the basis of this Agreement or (b) "Contractor" as defined in the County's Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement.

1.10. **"Contractor Confidential Information"** means all non-public proprietary information of Contractor that is marked confidential, restricted, proprietary, or with a similar designation; provided that Contractor Confidential Information excludes: (a) Using Agency Confidential Information, (b) Using Agency Data; (c) information that may be subject to disclosure under Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances; and (d) the terms of this Agreement, regardless of whether marked with a confidential designation or not.

1.11. **"Contractor Facilities"** means locations owned, leased or otherwise utilized by

Contractor and its Subcontractors from which it or they may provide Services.

1.12. **"Contractor Intellectual Property"** means all Intellectual Property owned or licensed by Contractor.

1.13. **"Contractor IP Materials"** means all IP Materials owned or licensed by Contractor.

1.14. **"Contractor Personnel"** means any individuals that are employees, representatives, Subcontractors or agents of Contractor, or of a direct or indirect Subcontractor of Contractor.

1.15. **"Contractor-Provided Equipment"** means Equipment provided by or on behalf of Contractor."

1.16. **"Contractor-Provided Software"** means Software provided by or on behalf of Contractor.

1.17. **"Criminal Justice Information"** means data that meets the definition of "Criminal Justice Information" in the most recent version of FBI's CJIS Security Policy and also data that meets the definition of "Criminal History Record Information" at 28 C.F.R. 20.

1.18. **"Critical Milestone"** means those milestones critical to the completion of the Services as identified in this Agreement, in any work plan, project plan, statement of work, or other document approved in advance by the Using Agency.

1.19. **"Data Protection Laws"** means laws, regulations, regulatory requirements, industry self-regulatory standards, and codes of practice in connection with the processing of Personal Information, including those provisions of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §§ 1320(d) et seq.) as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (42 U.S.C. §§ 17921 et seq.) and the Payment Card Industry standards.

1.20. **"Data Security Breach"** means (a) the loss or misuse (by any means) of any Using Agency Data or other Using Agency Confidential Information; (b) the unauthorized or unlawful access, use, or disclosure of any Using Agency Data or other Using Agency Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity or availability of any Using Agency Data or other Using Agency Confidential Information.

1.21. **"Deliverable"** has the same meaning as either: (a) "Deliverable" as defined in the County's Professional Services Agreement, if such document forms the basis of this Agreement; or (b) "Deliverable" as defined in the County's Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement. In either case, Deliverables includes without limitation Contractor-Provided Equipment, Contractor-Provided Software, Developed Intellectual Property.

1.22. **"Developed Intellectual Property"** means Intellectual Property as well as any IP Materials conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services, including, but not limited to: (a) modifications to, or enhancements (derivative works) of, the Using Agency Intellectual Property or the Using Agency IP Materials; (b) Developed Software; (c) documentation, training materials, or other IP Materials that do not modify or enhance then existing Using Agency IP Materials; and (d) modifications to or enhancements (derivative works) of, Third Party Intellectual Property or related IP Materials to the extent not owned by the

licensor of the Third Party Intellectual Property under the terms of the applicable license.

1.23. ***"Developed Software"*** any Software conceived, developed, authored or reduced to practice in the course of or in connection with the provision of the Services (including any modifications, enhancements, patches, upgrades or similar developments).

1.24. ***"Disaster"*** means a sudden, unplanned, calamitous event causing substantial damage or loss as defined or determined by a risk assessment and business impact analysis, and which creates an inability or substantial impairment on the organization's part to provide critical business functions for a material period of time. This also includes any period when the Using Agency management decides to divert resources from normal production responses and exercises its Disaster Recovery Plan.

1.25. ***"Disaster Recovery Plan"*** means the planned process, and related activities, required to return an IT environment to an acceptable condition of normal business operation following declaration of a Disaster.

1.26. ***"Equipment"*** means the computer, telecommunications, network, storage, and related hardware and peripherals owned or leased by the Using Agency or its Third Party Contractors, or by Contractor or its Subcontractors, and used or supported by Contractor or its Subcontractors, or by the Using Agency or its agents, in connection with the Services.

1.27. ***"Exit Assistance Plan"*** means a detailed plan for the delivery of the Exit Assistance Services.

1.28. ***"Exit Assistance Period"*** has the meaning given in Section 9.2.

1.29. ***"Exit Assistance Services"*** means such exit assistance services as are reasonably necessary from Contractor and/or its Subcontractors to enable a complete transition of the affected Services to the Using Agency or the Using Agency's designee(s), including, but not limited to, all of the services, tasks and functions described in Section 9.

1.30. ***"Illicit Code"*** means any hidden files, automatically replicating, transmitting or activating computer program, virus (or other harmful or malicious computer program) or any Equipment-limiting, Software-limiting or Services-limiting function (including, but not limited to, any key, node lock, time-out or similar function), whether implemented by electronic or other means.

1.31. ***"Incident"*** means any event that is not part of the standard operation of a service in the Using Agency IT environment (including an event in respect of the Services or any Equipment or Software) and that causes, or may cause, an interruption to, or a reduction in the quality of, that service. The Using Agency will determine the severity level of each reported Incident.

1.32. ***"Intellectual Property"*** means any inventions, discoveries, designs, processes, software, documentation, reports, and works of authorship, drawings, specifications, formulae, databases, algorithms, models, methods, techniques, technical data, discoveries, know how, trade secrets, and other technical proprietary information and all patents, copyrights, mask works, trademarks, service marks, trade names, service names, industrial designs, brand names, brand marks, trade dress rights, Internet domain name registrations, Internet web sites and corporate names, and applications for the registration or recordation of any of the foregoing.

1.33. **"IP Materials"** means works of authorship, software, documentation, processes, designs, drawings, specifications, formulae, databases, algorithms, models, methods, processes and techniques, technical data, inventions, discoveries, know how, the general format, organization, or structure of any report, document or database, and other technical proprietary information.

1.34. **"Laws"** means all United States federal, state and local laws or foreign laws, constitutions, statutes, codes, rules, regulations, ordinances, executive orders, decrees, edicts of or by any governmental authority having the force of law or any other legal requirement (including common law), including Data Protection Laws and the Cook County Code of Ordinances.

1.35. **"Open Source Materials"** means any Software that: (a) contains, or is derived in any manner (in whole or in part) from, any Software that is distributed as free Software, open source Software, shareware (e.g., Linux), or similar licensing or distribution models; and (b) is subject to any agreement with terms requiring that such Software be (i) disclosed or distributed in source code or object code form, (ii) licensed for the purpose of making derivative works, and/or (iii) redistributable. Open Source Materials includes without limitation "open source" code (as defined by the Open Source Initiative) and "free" code (as defined by the Free Software Foundation).

1.36. **"Party"** means either County, on behalf of County and its Using Agencies, or Contractor.

1.37. **"Parties"** means both County, on behalf of County and its Using Agencies, and Contractor.

1.38. **"Personal Information"** means personal data or information that relates to a specific, identifiable, individual person, including Using Agency personnel and individuals about whom the Using Agency, Contractor, Contractor's Subcontractors or affiliates has or collects financial and other information. For the avoidance of doubt, Personal Information includes the following: (a) any government-issued identification numbers (e.g., Social Security, driver's license, passport); (b) any financial account information, including account numbers, credit card numbers, debit card numbers, and other Cardholder Data; (c) Criminal Justice Information; (d) Protected Health Information; (e) user name or email address, in combination with a password or security question and answer that would permit access to an account; and (f) any other personal data defined as personally identifiable information under the breach notification laws of the fifty states.

1.39. **"Problem"** means the underlying cause of one or more Incidents, including where such cause is unknown or where it is known and a temporary work-around or permanent alternative has been identified.

1.40. **"Protected Health Information"** or PHI shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. 160.103.

1.41. **"Public Record"** shall have the same meaning as the term "public record" in the Illinois Local Records Act, 50 ILCS 205/1 et seq.

1.42. **"Required Consent"** means that consent required to secure any rights of use of or access to any of Using Agency-Provided Equipment, Using Agency-Provided Software, Using Agency Intellectual Property, Using Agency IP Materials, any other Equipment, any other Software whether Third Party Software or otherwise, any other Intellectual Property whether Third Party Intellectual Property or otherwise, any other IP Material, any of which are required by, requested by, used by or

accessed by Contractor, its Subcontractors, employees or other agents in connection with the Services.

1.43. **"Services"** either: (a) has the same meaning as "Services" as defined in Article 3 of the County's Professional Services Agreement, if such document forms the basis of this Agreement or (b) collectively means all of Contractor's services and other acts required in preparing, developing, and tendering the Using Agency's Deliverables as "Deliverables" is defined in the County's Instruction to Bidders and General Conditions, if such document forms the basis of this Agreement.

1.44. **"Service Level Agreements" or "SLA"** means service level requirement and is a standard for performance of Services, which sets Contractor and Using Agency expectations, and specifies the metrics by which the effectiveness of service activities, functions and processes will be measured, examined, changed and controlled.

1.45. **"Software"** means computer software, including source code, object, executable or binary code, comments, screens, user interfaces, data structures, data libraries, definition libraries, templates, menus, buttons and icons, and all files, data, materials, manuals, design notes and other items and documentation related thereto or associated therewith.

1.46. **"Third Party"** means a legal entity, company or person that is not a Party to the Agreement and is not a Using Agency, Subcontractor, affiliate of a Party, or other entity, company or person controlled by a Party.

1.47. **"Third Party Intellectual Property"** means all Intellectual Property owned by a Third Party, including Third Party Software.

1.48. **"Third Party Contractor"** means a Third Party that provides the Using Agency with products or services that are related to, or in support of, the Services. Subcontractors of Contractor are not "Third Party Contractors."

1.49. **"Third Party Software"** means a commercial Software product developed by a Third Party not specifically for or on behalf of the Using Agency. For clarity, custom or proprietary Software, including customizations to Third Party Software, developed by or on behalf of the Using Agency to the Using Agency's specifications shall not be considered Third Party Software.

1.50. **"Using Agency"** has the same meaning as the term "Using Agency" in the Cook County Procurement Code, located at Chapter 34, Article IV in the Cook County Code of Ordinances as amended, as applied to each department or agency receiving goods, Services or other Deliverables under this Agreement and includes Cook County, a body politic and corporate of the State of Illinois, on behalf of such Using Agency.

1.51. **"Using Agency Confidential Information"** means: (a) all non-public proprietary information of Using Agency that is marked confidential, restricted, proprietary, or with a similar designation; (b) Using Agency Data; and (c) any information that is exempt from public disclosure under the Illinois Freedom of Information Act, 5 ILCS 140/1 et seq. or under the Cook County Code of Ordinances.

1.52. **"Using Agency Data"** means all data, whether Personal Information or other data, provided by the Using Agency to Contractor, provided by Third Parties to Contractor for purposes relating to this Agreement, or otherwise encountered by Contractor for purposes relating to this

Agreement, including all data sent to Contractor by the Using Agency and/or stored by Contractor on any media relating to the Agreement, including metadata about such data. To the extent there is any uncertainty as to whether any data constitutes Using Agency Data, the data in question shall be treated as Using Agency Data. Using Agency Data further includes information that is: (a) input, processed or stored by the Using Agency's IT systems, including any Using Agency-Provided Software; (b) submitted to Contractor or its Subcontractors by any employees, agents, the Using Agency, Third Parties, business partners, and customers in connection with the Services or otherwise; (c) Incident records containing information relating to the Services; (d) Using Agency Intellectual Property and Using Agency IP Materials; (e) any raw data used to generate reports under this Agreement and any data included therein; and (f) Using Agency Confidential Information.

1.53. ***"Using Agency Intellectual Property"*** means all Intellectual Property owned or licensed by the Using Agency, including Developed Intellectual Property.

1.54. ***"Using Agency IP Materials"*** means all IP Materials owned or licensed by the Using Agency.

1.55. ***"Using Agency-Provided Equipment"*** means Equipment provided by or on behalf of Using Agency.

1.56. ***"Using Agency-Provided Software"*** means Software provided by or on behalf of Using Agency.

1.57. ***"WISP"*** means written information security program.

2. SERVICES AND DELIVERABLES

2.1. **Approved Facilities.** Contractor will perform Services only within the continental United States and only from locations owned, leased or otherwise utilized by Contractor and its Subcontractors.

2.2. **Licenses and Export Controls.** Contractor will be responsible for obtaining all necessary export authorizations and licenses for export of technical information or data relating to Using Agency Data, Software, Intellectual Property, IP Materials, or otherwise under this Agreement.

2.3. **Required Consents for Assets in Use and Third Party Contracts as of the Effective Date.** Contractor shall be responsible for obtaining all Required Consents relating to this Agreement. If Contractor is unable to obtain a Required Consent, Contractor shall implement, subject to the Using Agency's prior approval, alternative approaches as necessary to perform the Services. Contractor shall be responsible for and shall pay all costs associated with this section, including any fees or other charges imposed by the applicable Third Parties as a condition or consequence of their consent (*e.g.*, any transfer, upgrade or similar fees). The Using Agency shall cooperate with Contractor and provide Contractor such assistance in this regard as the Contractor may reasonably request.

2.4. **SLAs and Critical Milestones.** Commencing on the Effective Date or as otherwise specified in this Agreement, Contractor shall, as set forth in this Agreement: (a) perform the Services in accordance with SLAs and Critical Milestones; and (b) regularly measure and report on its performance against SLAs and Critical Milestones. Contractor shall maintain all data relating to and supporting the measurement of its performance, including performance against SLAs and Critical Milestones, in sufficient detail to permit a "bottom up" calculation, analysis and reconstruction of performance reports

(including all inclusion and exclusion calculations) throughout the term of this Agreement. Such data shall be made available to the Using Agency in an electronic format reasonably acceptable to the Using Agency upon reasonable request and upon the expiration or termination of this Agreement.

2.5. Default SLAs, Critical Milestones and Fee Reductions. Unless otherwise explicitly specified in this Agreement, the Contractor's SLAs, SLA targets, and Critical Milestones shall be those that the Using Agency recognizes as commonly accepted "industry best practices" for Services of similar cost, size, and criticality. For example and without limitation, such SLAs include availability and performance Contractor-Provided Software and hosting-related Services, on-time delivery of Deliverables, response and resolution times of Contractor's service desk. For example and without limitation, such Critical Milestones include significant events in projects such as completion of major Deliverables. Unless otherwise specified in this Agreement, Contractor shall proportionately reduce fees for failing to perform the Services in accordance with applicable SLAs and for failing to timely achieve Critical Milestones, and the Using Agency may withhold that amount of fee reduction from any outstanding Contractor invoice. Except as expressly allowed under this Agreement, any such fee reduction accompanying a failure to meet applicable SLAs or Critical Milestones shall not be the Using Agency's exclusive remedy and shall not preclude the Using Agency from seeking other remedies available to it for a material breach of this Agreement.

2.6. Standards and Procedures Manual. Contractor will prepare, update, and maintain a manual ("Standards and Procedures Manual") subject to the Using Agency's review and approval that shall: (a) be based upon ITIL processes and procedures; (b) conform to the Using Agency's standard operating procedures (c) be suitable to assist the Using Agency and the Using Agency's auditors in verifying and auditing the Contractor's performance of the Services; and (d) detail the operational and management processes by which Contractor will perform the Services under this Agreement, including to the extent applicable, processes relating to: (i) Change Management and Change control; (ii) Incident management; (iii) Problem management; (iv) configuration management; (v) backup and restore; (vi) capacity management and full utilization of resources; (vii) project management; (viii) management information; (ix) security processes; (x) Contractor's Business Continuity Plan; (xi) Contractor's Disaster Recovery Plan; and (xi) administration, including invoicing. Where this Agreement assumes that the Using Agency will provide Tier 1 help desk support, the Standards and Procedures Manual shall also include sufficient help desk scripts for the Using Agency to provide such support. Contractor will perform the Services in accordance with the Standards and Procedures Manual; *provided, however*, that the provisions of the Standards and Procedures Manual shall never supersede the provisions of this Agreement.

2.7. Project Management Methodology. Contractor shall perform the Services in accordance with an industry-recognized project management methodology and procedures, subject to Using Agency approval. Contractor shall comply with the Using Agency's procedures for tracking progress and documents for the duration of the Agreement, including the submission of weekly or monthly status reports to the Using Agency as the Using Agency may require.

2.8. Change Management Procedures. Contractor shall utilize Change Management procedures, subject to Using Agency approval, that conform to ITIL/ITSM to manage, track and report on Changes relating to the Services, including procedures for scheduling maintenance, patching, replacement of assets, and other matters required for proper management of the Services. No Change will be made without the Using Agency's prior written consent (which may be given or withheld in the Using Agency's sole discretion), unless such Change: (a) has no impact on the Services being provided by

Contractor; (b) has no impact on the security of the Using Agency Data and the Using Agency systems; and (c) causes no increase in any fees under this Agreement or the Using Agency's retained costs.

2.9. Resources Necessary for Services. Except as set forth in this Agreement, Contractor shall provide and be financially responsible for all Equipment, Software, materials, facilities, systems and other resources needed to perform the Services in accordance with the Agreement.

2.10. Using Agency Resources. Except as explicitly allowed under this Agreement, Contractor shall not use, nor permit any Subcontractor, employee, agent, or other Third Party to use any Using Agency-Provided Equipment, Using Agency-Provided Software, Using Agency facilities, or any other Equipment, Software, materials, facilities, systems or other resources that the Using Agency provides or otherwise makes available under this Agreement for any purpose other than the performance of the Services; and Contractor shall do so only upon prior written approval of the Using Agency. Contractor shall not purport to, pledge or charge by way of security any of the aforementioned. Contractor shall keep any Equipment owned or leased by the Using Agency that is under Contractor's or a Contractor Subcontractor's control, secure and, for any such Equipment that is not located at the Using Agency facilities, such Equipment shall be clearly identified as the Using Agency's and separable from Contractor's and Third Parties' property.

2.11. Maintenance of Assets. Contractor shall maintain all Equipment, Software, materials, systems, and other resources utilized predominately or exclusively for performing Services in good condition, less ordinary wear and tear, and in such locations and configurations as to be readily identifiable.

2.12. Service Compatibility. To the extent necessary to provide the Services, Contractor shall ensure that the Services, Contractor-Provided Equipment and Contractor-Provided Software (collectively, the "Contractor Resources") are interoperable with the Using Agency-Provided Equipment, Using Agency-Provided Software and with the Using Agency's other Assets, at no cost beyond that specified in this Agreement and without adversely affecting any systems or services retained by the Using Agency or its Third Party Contractors. In the event of any Problem related to service compatibility where it is not known whether the Problem is caused by Contractor's Assets or by Using Agency's Assets, Contractor shall be responsible for correcting the Problem except to the extent that Contractor can demonstrate, to the Using Agency's satisfaction, that the cause was not due to Contractor Resources or to Contractor's action or inaction.

2.13. Cooperation with Using Agency's Third Party Contractors. Contractor shall cooperate with all Third Party Contractors to coordinate its performance of the Services with the services and systems of such Third Party Contractors. Subject to reasonable confidentiality requirements, such cooperation shall include providing: (a) applicable written information, standards and policies concerning any or all of the systems, data, computing environment, and technology direction used in performing the Services so that the goods and services provided by the Third Party Contractor may work in conjunction with or be integrated with the Services; (b) assistance and support services to such Third Party Contractors; (c) Contractor's quality assurance, its development and performance acceptance testing and the applicable requirements of any necessary interfaces for the Third Party Contractor's work product; (d) applicable written requirements of any necessary modifications to the systems or computing environment; and (e) access to and use of the Contractor's Assets as mutually agreed upon by the Using Agency and Contractor (such agreement not to be unreasonably withheld or delayed) and subject to the Third Party Contractor's agreement to comply with Contractor's applicable standard

security policies.

2.14. Procurement Assistance. At any time during the Agreement, Contractor shall, as requested by the Using Agency, reasonably cooperate and assist the Using Agency with any Using Agency procurement relating to any of the Services or replacing the Services, including: (a) providing information, reports and data for use in the Using Agency's procurement or transition to a subsequent Third Party Contractor; (b) answering Third Parties' and Using Agency's questions regarding the procurement and Services transition; and (c) allowing Third Parties participating in the Using Agency's procurement to perform reasonable, non-disruptive due diligence activities in respect of the relevant Services, including providing reasonable access to Key Personnel.

3. WARRANTIES

3.1. Compliance with Law and Regulations. Contractor represents and warrants that it shall perform its obligations under this Agreement in accordance with all Laws applicable to Contractor and its business, including Laws applicable to the manner in which the Services are performed, including any changes in such Laws. With respect to laws governing data security and privacy, the term 'Contractor Laws' shall include any Laws that would be applicable to Contractor if it, rather than the Using Agency, were the owner or data controller of any of the Using Agency Data in its possession or under its control in connection with the Services. Contractor also represents and warrants that it shall identify, obtain, keep current, and provide for Contractor's inspection, all necessary licenses, approvals, permits, authorizations, visas and the like as may be required from time to time under Contractor Laws for Contractor to perform the Services.

3.2. Non-Infringement. Contractor represents and warrants that it shall perform its responsibilities under this Agreement in a manner that does not infringe any patent, copyright, trademark, trade secret or other proprietary rights of any Third Party.

3.3. Contractor Materials and Third Party Intellectual Property. Contractor represents and warrants that it owns, or is authorized to use, all Contractor Intellectual Property, Contractor IP Materials and Contractor-provided Third Party Intellectual Property.

3.4. Developed Software. Contractor represents and warrants that all Developed Software shall be free from material errors in operation and performance, shall comply with the applicable documentation and specifications in all material respects, for twelve (12) months after the installation, testing and acceptance of such Developed Software by the Using Agency; provided, however, for Developed Software that executes on a monthly or less frequent basis (e.g., quarterly or annual cycle), such warranty period will commence on the date of first execution of such Software. Any repairs made to Developed Software pursuant to this Section shall receive a new twelve (12) month warranty period in accordance with the terms of this Section.

3.5. No Open Source. Contractor represents and warrants that Contractor has not (i) incorporated Open Source Materials into, or combined Open Source Materials with, the Deliverables or Software, (ii) distributed Open Source Materials in conjunction with any Deliverables or Software, or (iii) used Open Source Materials, in such a way that, with respect to the foregoing (i), (ii), or (iii), creates obligations for the Contractor with respect to any material Deliverables or grant, or purport to grant, to any Third Party, any rights or immunities under any material Deliverables (including, but not limited to, using any Open Source Materials that require, as a condition of use, modification and/or distribution of such Open Source Materials that other material Software included in Deliverables incorporated into,

derived from or distributed with such Open Source Materials be (A) disclosed or distributed in source code form, (B) be licensed for the purpose of making derivative works, or (C) be redistributable at no charge).

3.6. Access to Using Agency Data. Contractor represents and warrants that Contractor has not and will not prevent, or reasonably fail to allow, for any reason including without limitation late payment or otherwise, the Using Agency's access to and retrieval of Using Agency Data. Contractor acknowledges that Using Agency Data may be Public Records and that any person who knowingly, without lawful authority and with the intent to defraud any party, public officer, or entity, alters, destroys, defaces, removes, or conceals any Public Record commits a Class 4 felony.

3.7. Viruses. Contractor represents and warrants that it has not knowingly provided, and will not knowingly provide, to the Using Agency in connection with the Services, any Software that uses Illicit Code. Contractor represents and warrants that it has not and will not introduce, invoke or cause to be invoked such Illicit Code in any Using Agency IT environment at any time, including upon expiration or termination of this Agreement for any reason, without the Using Agency's prior written consent. If Contractor discovers that Illicit Code has been introduced into Software residing on Equipment hosted or supported by Contractor, Contractor shall, at no additional charge, (a) immediately undertake to remove such Illicit Code, (b) promptly notify the Using Agency in writing of the introduction, and (c) use reasonable efforts to correct and repair any damage to Using Agency Data or Software caused by such Illicit Code and otherwise assist the Using Agency in mitigating such damage and restoring any affected Service, Software or Equipment.

3.8. Resale of Equipment and Software. If Contractor resells to the Using Agency any Equipment or Software that Contractor purchased from a Third Party, then Contractor, to the extent it is legally able to do so, shall pass through any such Third Party warranties to the Using Agency and reasonably cooperate in enforcing them. Such warranty pass-through will not relieve Contractor from its warranty obligations set forth in this Section.

3.9. Data Security. Contractor warrants and represents that (i) the performance of the Services shall not permit any unauthorized access to or cause any loss or damage to Using Agency Data, Using Agency Intellectual Property, or other Using Agency Confidential Information; and (ii) it complies and shall comply with all Using Agency security policies in place from time to time during the term of this Agreement.

4. INTELLECTUAL PROPERTY

4.1. Using Agency Intellectual Property. The Using Agency retains all right, title and interest in and to all Using Agency Intellectual Property and Using Agency IP Materials. To the extent the Using Agency may grant such license, Contractor is granted a worldwide, fully paid-up, nonexclusive license during the term of this Agreement to use, copy, maintain, modify, enhance and create derivative works of the Using Agency Intellectual Property and Using Agency IP Materials that are necessary for performing the Services, and that are explicitly identified in writing by the Using Agency's Chief Information Officer, for the sole purpose of performing the Services pursuant to this Agreement. Contractor shall not be permitted to use any of the Using Agency Intellectual Property or Using Agency IP Materials for the benefit of any entities other than the Using Agency. Contractor shall cease all use of the Using Agency Intellectual Property and Using Agency IP Materials upon expiration or termination of this Agreement. Upon expiration or termination of this Agreement or relevant Services under this

Agreement, Contractor shall return to the Using Agency all the Using Agency Intellectual Property, Using Agency IP Materials and copies thereof possessed by Contractor.

4.2. Developed Intellectual Property. As between the Parties, the Using Agency shall have all right, title and interest in all Developed Intellectual Property. Contractor hereby irrevocably and unconditionally assigns, transfers and conveys to the Using Agency without further consideration all of its right, title and interest in such Developed Intellectual Property, including all rights of patent, copyright, trade secret or other proprietary rights in such materials, which assignment shall be effective as of the creation of such works without need for any further documentation or action on the part of the Parties. Contractor agrees to execute any documents or take any other actions as may reasonably be necessary, or as the Using Agency may reasonably request, to perfect the Using Agency's ownership of any such Developed Intellectual Property. Contractor shall secure compliance with this Section by any personnel, employees, contractors or other agents of Contractor and its Subcontractors involved directly or indirectly in the performance of Services under this Agreement.

4.3. Contractor Intellectual Property. Contractor retains all right, title and interest in and to Contractor Intellectual Property and Contractor IP Materials that Contractor developed before or independently of this Agreement. Contractor grants to the Using Agency, a fully-paid, royalty-free, non-exclusive, non-transferable, worldwide, irrevocable, perpetual, assignable license to make, have made, use, reproduce, distribute, modify, publicly display, publicly perform, digitally perform, transmit, copy, and create derivative works based upon Contractor Intellectual Property and Contractor IP Materials, in any media now known or hereafter known, to the extent the same are embodied in the Services and Deliverables, or otherwise required to exploit the Services or Deliverables. During the term of this Agreement and immediately upon any expiration or termination thereof for any reason, Contractor will provide to the Using Agency the most current copies of any Contractor IP Materials to which the Using Agency has rights pursuant to the foregoing, including any related documentation. Contractor bears the burden to prove that Intellectual Property and IP Materials related to this Agreement were not created under this Agreement.

4.4. Third Party Intellectual Property. Contractor shall not introduce into the Using Agency's environment any Third Party Intellectual Property or otherwise use such Third Party Intellectual Property to perform the Services without first obtaining the prior written consent from the Using Agency's Chief Information Officer, which the Using Agency may give or withhold in its sole discretion. A decision by the Using Agency to withhold its consent shall not relieve Contractor of any obligation to perform the Services.

4.5. Residual Knowledge. Nothing contained in this Agreement shall restrict either Contractor or Using Agency from the use of any ideas, concepts, know-how, methodologies, processes, technologies, algorithms or techniques relating to the Services which either Contractor or Using Agency, individually or jointly, develops or discloses under this Agreement, provided that in doing so Contractor or Using Agency does not breach its respective obligations under Section 5 relating to confidentiality and non-disclosure and does not infringe the Intellectual Property rights of the other or Third Parties who have licensed or provided materials to the other. Except for the license rights contained under Section 4, neither this Agreement nor any disclosure made hereunder grants any license to either Contractor or Using Agency under any Intellectual Property rights of the other.

4.6. Software Licenses. This Agreement contains all terms and conditions relating to all licenses in Contractor-Provided Software and Contractor IP Materials. Except as explicitly set forth

elsewhere in this Agreement, all licenses that Contractor grants in Contractor-Provided Software include the right of use by Third Party Contractors for the benefit of the Using Agency, the right to make backup copies for backup purposes or as may be required by the Using Agency's Business Continuity Plan or Disaster Recovery Plan, the right to reasonably approve the procedures by which Contractor may audit the use of license entitlements, and the right to give reasonable approval before Contractor changes Contractor-Provided Software in a manner that materially and negatively impacts the Using Agency.

5. USING AGENCY DATA AND CONFIDENTIALITY

5.1. Property of Using Agency. All Using Agency Confidential Information, including without limitation Using Agency Data, shall be and remain the sole property of the Using Agency. Contractor shall not utilize the Using Agency Data or any other Using Agency Confidential Information for any purpose other than that of performing the Services under this Agreement. Contractor shall not, and Contractor shall ensure that its Subcontractors, its employees, or agents do not, possess or assert any lien or other right against or to the Using Agency Data or any other Using Agency Confidential Information. Without the Using Agency's express written permission, which the Using Agency may give or withhold in its sole discretion, no Using Agency Data nor any other Using Agency Confidential Information, or any part thereof, shall be disclosed, shared, sold, assigned, leased, destroyed, altered, withheld, or otherwise restricted of by Contractor or commercially exploited by or on behalf of Contractor, its employees, Subcontractors or agents.

5.2. Acknowledgment of Importance of Using Agency Confidential Information. Contractor acknowledges the importance of Using Agency Confidential Information, including without limitation Using Agency Data, to the Using Agency and, where applicable, Third Party proprietors of such information, and recognizes that the Using Agency and/or Third Party proprietors may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Agreement.

5.3. Return of Using Agency Data and Other Using Agency Confidential Information. Upon the Using Agency's request, at any time during this Agreement or at termination or expiration of this Agreement, Contractor shall promptly return any and all requested Using Agency Data and all other requested Using Agency Confidential Information to the Using Agency or its designee in such a format as the Using Agency may reasonably request. Contractor shall also provide sufficient information requested by the Using Agency about the format and structure of the Using Agency Data to enable such data to be used in substantially the manner in which Contractor utilized such data. Also upon Using Agency's request, in lieu of return or in addition to return, Contractor shall destroy Using Agency Data and other Using Agency Confidential Information, sanitize any media upon which such the aforementioned resided using a process that meets or exceeds DoD 5220.28-M 3-pass specifications, and provide documentation of same within 10 days of completion, all in compliance with Using Agency's policies and procedures as updated. All other materials which contain Using Agency Data and other Using Agency Confidential Information shall be physically destroyed and shredded in accordance to NIST Special Publication 800-88; and upon Using Agency request, Contractor shall provide Using Agency with a certificate of destruction in compliance with NIST Special Publication 800-88. Contractor shall be relieved from its obligation to perform any Service to the extent the return of any Using Agency Data or other Using Agency Confidential Information at the Using Agency's request under this Section materially impacts Contractor's ability to perform such Service; provided, that Contractor gives the Using Agency notice of the impact of the return and continues to use reasonable efforts to perform.

5.4. Public Records. Contractor will adhere to all Laws governing Public Records located at 50 ILCS 205/1 et seq. and at 44 Ill. Admin. Code 4500.10 et seq. Specifically, and without limitation, Contractor shall: (a) store Using Agency Data in such a way that each record is individually accessible for the length of the Using Agency's scheduled retention; (b) retain a minimum of two total copies of all Using Agency Data; (c) retain Using Agency Data according to industry best practices for geographic redundancy, such as NIST Special Publication 800-34 as revised; (d) store and access Using Agency Data in a manner allowing individual records to maintain their relationships with one another; (e) capture relevant structural, descriptive, and administrative metadata to Using Agency Data at the time a record is created or enters the control of Contractor or its Subcontractors.

5.5. Disclosure Required by Law, Regulation or Court Order. In the event that Contractor is required to disclose Using Agency Data or other Using Agency Confidential Information in accordance with a requirement or request by operation of Law, regulation or court order, Contractor shall, except to the extent prohibited by law: (a) advise the Using Agency thereof prior to disclosure; (b) take such steps to limit the extent of the disclosure to the extent lawful and reasonably practical; (c) afford the Using Agency a reasonable opportunity to intervene in the proceedings; and (d) comply with the Using Agency's requests as to the manner and terms of any such disclosure.

5.6. Loss of Using Agency Confidential Information. Without limiting any rights and responsibilities under Section 7 of these IT Special Conditions, in the event of any disclosure or loss of, or inability to account for, any Using Agency Confidential Information, Contractor shall promptly, at its own expense: (a) notify the Using Agency in writing; (b) take such actions as may be necessary or reasonably requested by the Using Agency to minimize the violation; and (c) cooperate in all reasonable respects with the Using Agency to minimize the violation and any damage resulting therefrom.

5.6. Undertakings With Respect To Personnel. Contractor acknowledges and agrees that it is responsible for the maintenance of the confidentiality of Using Agency Data and other Using Agency Confidential Information by Contractor Personnel. Without limiting the generality of the foregoing, Contractor shall undertake to inform all Contractor Personnel of Contractor's obligations with respect to Using Agency Data and other Using Agency Confidential Information and shall undertake to ensure that all Contractor Personnel comply with Contractor's obligations with respect to same.

5.7. Background Checks of Contractor Personnel. Whenever the Using Agency deems it reasonably necessary for security reasons, the Using Agency or its designee may conduct, at its expense, criminal and driver history background checks of Contractor Personnel. Contractor and its Subcontractors shall immediately reassign any individual who, in the opinion of the Using Agency, does not pass the background check.

5.8. Contractor Confidential Information. Using Agency shall use at least the same degree of care to prevent disclosing Contractor Confidential Information to Third Parties as Using Agency employs to avoid unauthorized disclosure, publication or dissemination of its Using Agency Confidential Information of like character.

6. DATA SECURITY AND PRIVACY

6.1. General Requirement of Confidentiality and Security. It shall be Contractor's obligation to maintain the confidentiality and security of all Using Agency Confidential Information, including without limitation Using Agency Data, in connection with the performance of the Services. Without limiting Contractor's other obligations under this Agreement, Contractor shall implement and/or use

network management and maintenance applications and tools and appropriate fraud prevention and detection and encryption technologies to protect the aforementioned; provided that Contractor shall, at a minimum, encrypt all Personal Information in-transit and at-rest. Contractor shall perform all Services utilizing security technologies and techniques and in accordance with industry leading practices and the Using Agency's security policies, procedures and other requirements made available to Contractor in writing, including those relating to the prevention and detection of fraud or other inappropriate use or access of systems and networks.

6.2. General Compliance. Contractor shall comply with all applicable Laws, regulatory requirements and codes of practice in connection with all capturing, processing, storing and disposing of Personal Information by Contractor pursuant to its obligations under this Agreement and applicable Data Protection Laws and shall not do, or cause or permit to be done, anything that may cause or otherwise result in a breach by the Using Agency of the same. Contractor and all Contractor Personnel shall comply with all the Using Agency policies and procedures regarding data access, privacy and security.

6.3. Security. Contractor shall establish and maintain reasonable and appropriate physical, logical, and administrative safeguards to preserve the security and confidentiality of the Using Agency Data and other Using Agency Confidential Information and to protect same against unauthorized or unlawful disclosure, access or processing, accidental loss, destruction or damage. Such safeguards shall be deemed reasonable and appropriate if established and maintained with the more rigorous of: (a) the Using Agency Policies as updated; (b) the security standards employed by Contractor with respect to the protection of its confidential information and trade secrets as updated; (c) security standards provided by Contractor to its other customers at no additional cost to such customers, as updated; or (d) compliance with the then-current NIST 800-series standards and successors thereto or an equivalent, generally accepted, industry-standard security standards series.

6.4. Written Information Security Program. Contractor shall establish and maintain a WISP designed to preserve the security and confidentiality of the Using Agency Data and other Using Agency Confidential Information. Contractor's WISP shall include Data Breach procedures and annual Data Breach response exercises. Contractor's WISP shall be reasonably detailed and shall be subject to the Using Agency's reasonable approval.

6.5. Contractor Personnel. Contractor will oblige its Contractor Personnel to comply with applicable Data Protection Laws and to undertake only to collect, process or use any Using Agency Data, Using Agency Intellectual Property, Using Agency Confidential Information, or Personal Information received from or on behalf of the Using Agency for purposes of, and necessary to, performing the Services and not to make the aforementioned available to any Third Parties except as specifically authorized hereunder. Contractor shall ensure that, prior to performing any Services or accessing any Using Agency Data or other Using Agency Confidential Information, all Contractor Personnel who may have access to the aforementioned shall have executed agreements concerning access protection and data/software security consistent with this Agreement.

6.6. Information Access. Contractor shall not attempt to or permit access to any Using Agency Data or other Using Agency Confidential Information by any unauthorized individual or entity. Contractor shall provide each of the Contractor Personnel, Subcontractors and agents only such access as is minimally necessary for such persons/entities to perform the tasks and functions for which they are responsible. Contractor shall, upon request from the Using Agency, provide the Using Agency with an

updated list of those Contractor Personnel, Subcontractors and agents having access to Using Agency Data and other Using Agency Confidential Information and the level of such access. Contractor shall maintain written policies that include auditing access levels and terminating access rights for off-boarded Contractor Personnel, Subcontractors and agents.

6.7. Protected Health Information. If Contractor will have access to Personal Health Information in connection with the performance of the Services, Contractor shall execute a Business Associate Agreement in a form provided by the Using Agency.

6.8. Criminal Justice Information. If Contractor will have access to Criminal Justice Information in connection with the performance of the Services, Contractor shall execute an addendum to this Agreement governing the Contractor's access to such Criminal Justice Information in a form provided by the Using Agency.

6.9. Cardholder Data. If Contractor will have access to Cardholder Data in connection with the performance of the Services, no less than annually, Contractor shall tender to Using Agency a current attestation of compliance signed by a Qualified Security Assessor certified by the Payment Card Industry.

6.10. Encryption Requirement. Contractor shall encrypt all Personal Information and all other Using Agency Confidential Information the disclosure of which would reasonably threaten the confidentiality and security of Using Agency Data. Contractor shall encrypt the aforementioned in motion, at rest and in use in a manner that, at a minimum, adheres to NIST SP 800-111, NIST SP 800-52, NIST SP 800-77 and NIST SP 800-113 encryption standards. Contractor shall not deviate from this encryption requirement without the advance, written approval of the Using Agency's Information Security Office.

6.11. Using Agency Security. Contractor shall notify the Using Agency if it becomes aware of any Using Agency security practices or procedures (or any lack thereof) that Contractor believes do not comport with generally accepted security policies or procedures.

6.12. Contractor as a Data Processor. Contractor understands and acknowledges that, to the extent that performance of its obligations hereunder involves or necessitates the processing of Personal Information, it shall act only on instructions and directions from the Using Agency; *provided, however,* that Contractor shall notify the Using Agency if it receives instructions or directions from the Using Agency that Contractor believes do not comport with generally accepted security policies or procedures and the Using Agency shall determine whether to modify such instructions or have Contractor comply with such instructions unchanged.

6.13. Data Subject Right of Access and Rectification. If the Using Agency is required to provide or rectify information regarding an individual's Personal Information, Contractor will reasonably cooperate with the Using Agency to the full extent necessary to comply with Data Protection Laws. If a request by a data subject is made directly to Contractor, Contractor shall notify the Using Agency of such request as soon as reasonably practicable.

6.14. Security, Privacy and Data Minimization in Software Development Life Cycle. Contractor shall implement an industry-recognized procedure that addresses the security and privacy of Personal Information as part of the software development life cycle in connection with the performance of the Services. Contractor shall implement procedures to minimize the collection of Personal Information and

shall, subject to Using Agency's written request to the contrary, minimize the collection of Personal Information.

6.15. Advertising and Sale of Using Agency Data. Nothing in this Agreement shall be construed to limit or prohibit a Using Agency's right to advertise, sell or otherwise distribute Using Agency Data as permitted by the Cook County Code of Ordinances.

7. DATA SECURITY BREACH

7.1. Notice to Using Agency. Contractor shall provide to the Using Agency written notice of such Data Security Breach promptly following, and in no event later than one (1) business day following, the discovery or suspicion of the occurrence of a Data Security Breach. Such notice shall summarize in reasonable detail the nature of the Using Agency Data that may have been exposed, and, if applicable, any persons whose Personal Information may have been affected, or exposed by such Data Security Breach. Contractor shall not make any public announcements relating to such Data Security Breach without the Using Agency's prior written approval.

7.2. Data Breach Responsibilities. If Contractor knows or has reason to know that a Data Security Breach has occurred (or potentially has occurred), Contractor shall: (a) reasonably cooperate with the Using Agency in connection with the investigation of known and suspected Data Security Breaches; (b) perform any corrective actions that are within the scope of the Services; and (c) at the request and under the direction of the Using Agency, take any all other remedial actions that the Using Agency deems necessary or appropriate, including without limitation, providing notice to all persons whose Personal Information may have been affected or exposed by such Data Security Breach, whether or not such notice is required by Law.

7.3. Data Breach Exercises. Contractor shall conduct annual Data Breach exercises. Upon Using Agency request, Contractor shall coordinate its exercises with the Using Agency.

7.4. Costs. The costs incurred in connection with Contractor's obligations set forth in Section 7 or Using Agency's obligations under relevant Data Security Laws shall be the responsibility of the Party whose acts or omissions caused or resulted in the Data Security Beach and may include without limitation: (a) the development and delivery of legal notices or reports required by Law, including research and analysis to determine whether such notices or reports may be required; (b) examination and repair of Using Agency Data that may have been altered or damaged in connection with the Data Security Breach, (c) containment, elimination and remediation of the Data Security Breach, and (d) implementation of new or additional security measures reasonably necessary to prevent additional Data Security Breaches; (e) providing notice to all persons whose Personal Information may have been affected or exposed by such Data Security Breach, whether or required by Law; (f) the establishment of a toll-free telephone number, email address, and staffing of corresponding communications center where affected persons may receive information relating to the Data Security Breach; (g) the provision of one (1) year of credit monitoring/repair and/or identity restoration/insurance for affected persons.

8. AUDIT RIGHTS

8.1. Generally. Contractor and its Subcontractors shall provide access to any records, facilities, personnel, and systems relating to the Services, at any time during standard business hours, to the Using Agency and its internal or external auditors, inspectors and regulators in order to audit, inspect, examine, test, and verify: (a) the availability, integrity and confidentiality of Using Agency Data

and examine the systems that process, store, support and transmit Using Agency Data; (b) controls placed in operation by Contractor and its Subcontractors relating to Using Agency Data and any Services; (c) Contractor's disaster recovery and backup/recovery processes and procedures; and (d) Contractor's performance of the Services in accordance with the Agreement. The aforementioned Using Agency audit rights include the Using Agency's right to verify or conduct its own SOC 2 audits.

8.2. Security Audits. Contractor shall perform, at its sole cost and expense, a security audit no less frequently than every twelve (12) months. The security audit shall test Contractor's compliance with security standards and procedures set forth in: (a) this Agreement, (b) the Standards and Procedures Manual, and (c) any security standards and procedures otherwise agreed to by the Parties.

8.3. Service Organization Control (SOC 2), Type II Audits. Contractor shall, at least once annually in the fourth (4th) calendar quarter and at its sole cost and expense, provide to the Using Agency and its auditors a Service Organization Control (SOC 2), Type II report for all locations at which the Using Agency Data is processed or stored.

8.4. Audits Conducted by Contractor. Contractor promptly shall make available to the Using Agency the results of any reviews or audits conducted by Contractor and its Subcontractors, agents or representatives (including internal and external auditors), including SOC 2 audits, relating to Contractor's and its Subcontractors' operating practices and procedures to the extent relevant to the Services or any of Contractor's obligations under the Agreement. To the extent that the results of any such audits reveal deficiencies or issues that impact the Using Agency or the Services, Contractor shall provide the Using Agency with such results promptly following completion thereof.

8.5. Internal Controls. Contractor shall notify the Using Agency prior to modifying any of its internal controls that impact the Using Agency, the Services and/or Using Agency Data and shall demonstrate compliance with this Agreement.

8.6. Subcontractor Agreements. Contractor shall ensure that all agreements with its Subcontractors performing Services under this Agreement contain terms and conditions consistent with the Using Agency's audit rights.

9. RIGHT TO EXIT ASSISTANCE

9.1. Payment for Exit Assistance Services. Exit Assistance Services shall be deemed a part of the Services and included within the Contractor's fees under this Agreement, except as otherwise detailed in this Agreement.

9.2. General. Upon Using Agency's request in relation to any termination, regardless of reason, or expiration of the Agreement, in whole or in part, Contractor shall provide the Using Agency and each of its designees Exit Assistance Services. During the Exit Assistance Period, Contractor shall continue to perform the terminated Services except as approved by the Using Agency and included in the Exit Assistance Plan. Contractor's obligation to provide the Exit Assistance Services shall not cease until the Services have been completely transitioned to the Using Agency or the Using Agency's designee(s) to the Using Agency's satisfaction.

9.3. Exit Assistance Period. Contractor shall: (a) commence providing Exit Assistance Services at the Using Agency's request (i) up to six (6) months prior to the expiration of the Agreement,

or (ii) in the event of termination of the Agreement or any Services hereunder, promptly following receipt of notice of termination from the Party giving such notice (such date notice is received, the "Termination Notice Date"), and (b) continue to provide the Exit Assistance Services through the effective date of termination or expiration of the Agreement or the applicable terminated Services (as applicable, the "Termination Date") (such period, the "Exit Assistance Period"). At the Using Agency's option, the Exit Assistance Period may be extended for a period of up to twelve (12) months after the Termination Date. The Using Agency shall provide notice regarding its request for Exit Assistance Services at least sixty (60) days prior to the date upon which the Using Agency requests that Contractor commence Exit Assistance Services unless such time is not practicable given the cause of termination.

9.4. Manner of Exit Assistance Services. Contractor shall perform the Exit Assistance Services in a manner that, to the extent the same is within the reasonable control of Contractor: (a) is in accordance with the Using Agency's reasonable direction; (b) is in cooperation with, and causes its Subcontractors to cooperate with, the Using Agency and the Using Agency's designee(s); (c) supports the efficient and orderly transfer of the terminated Services to the Using Agency; (d) minimizes any impact on the Using Agency's operations; (e) minimizes any internal and Third Party costs incurred by the Using Agency and the Using Agency's designee(s); and (f) minimizes any disruption or deterioration of the terminated Services. Exit Assistance Plan. Contractor shall develop and provide to the Using Agency, subject to the Using Agency's approval and authorization to proceed, an Exit Assistance Plan that shall: (a) describe responsibilities and actions to be taken by Contractor in performing the Exit Assistance Services; (b) describe in detail any Using Agency Responsibilities which are necessary for Contractor to perform the Exit Assistance Services; (c) describe how any transfer of Assets and any novation, assignment or transfer of contracts will be achieved during the Exit Assistance Period; (d) detail the return, and schedule for return, of Using Agency Data and other Using Agency-specific information to be provided; (e) set out the timetable for the transfer of each element of the terminated Services (including key milestones to track the progress); (f) identify a responsible party for each service, task and responsibility to be performed under the Exit Assistance Plan; and (g) specify reasonable acceptance criteria and testing procedures to confirm whether the transfer of the terminated Services has been successfully completed. Following the Using Agency's approval of, and authorization to proceed with the final Exit Assistance Plan, Contractor will perform the Exit Assistance Services in accordance with the Exit Assistance Plan.

9.6. Exit Assistance Management. Within the first thirty (30) days of the Exit Assistance Period, Contractor will appoint a senior project manager to be responsible for, and Contractor's primary point of contact for, the overall performance of the Exit Assistance Services. Upon Using Agency request, Contractor will provide individuals with the required expertise to perform Exit Assistance Services, even if those individuals are not currently performing Services. Contractor will promptly escalate to the Using Agency any failures (or potential failures) regarding the Exit Assistance Services. Contractor will meet weekly with the Using Agency and provide weekly reports describing: the progress of the Exit Assistance Services against the Exit Assistance Plan; any risks encountered during the performance of the Exit Assistance Services; and proposed steps to mitigate such risks. The Using Agency may appoint, during the Exit Assistance Period, a Using Agency designee to be the Using Agency's primary point of contact and/or to operationally manage Contractor during the Exit Assistance Period.

9.7. Removal of Contractor Materials. Contractor shall be responsible at its own expense for de-installation and removal from the Using Agency Facilities any Equipment owned or leased by Contractor that is not being transferred to the Using Agency under the Agreement subject to the Using

Agency's reasonable procedures and in a manner that minimizes the adverse impact on the Using Agency. Prior to removing any documents, equipment, software or other material from any Using Agency Facility, Contractor shall provide the Using Agency with reasonable prior written notice identifying the property it intends to remove. Such identification shall be in sufficient detail to apprise the Using Agency of the nature and ownership of such property.

9.8. Using Agency-specific Information. Upon Using Agency's request, Contractor will specifically provide to the Using Agency the following Using Agency Data to relating to the Services: (a) SLA statistics, reports and associated raw data; (b) operational logs; (c) the Standards and Procedures Manual; (d) Incident and Problem logs for at least the previous two (2) years; (e) security features; (f) passwords and password control policies; (g) identification of work planned or in progress as of the Termination Date, including the current status of such work and projects; and (h) any other information relating to the Services or the Using Agency's IT or operating environment which would be required by a reasonably skilled and experienced Contractor of services to assume and to continue to perform the Services following the Termination Date without disruption or deterioration. This section shall not limit any other rights and duties relating to Using Agency Data.

9.9. Subcontractors and Third Party Contracts. For each contract for which Using Agency has an option to novate or transfer, Contractor will supply the following information upon Using Agency's request: (a) description of the goods or service being provided under the contract; (b) whether the contract exclusively relates to the Services; (c) whether the contract can be assigned, novated or otherwise transferred to the Using Agency or its designee and any restrictions or costs associated with such a transfer; (d) the licenses, rights or permissions granted pursuant to the contract by the Third Party; (e) amounts payable pursuant to the terms of such contract; (f) the remaining term of the contract and termination rights; and (g) contact details of the Third Party. Contractor's agreements with Third Parties that predominantly or exclusively relate to this Agreement shall not include any terms that would restrict such Third Parties from entering into agreements with the Using Agency or its designees as provided herein.

9.10. Knowledge Transfer. As part of the Exit Assistance Services and upon Using Agency's reasonable request, Contractor will provide knowledge transfer services to the Using Agency or the Using Agency's designee to allow the Using Agency or such designee to fully assume, become self-reliant with respect to, and continue without interruption, the provision of the terminated Services. Contractor shall: allow personnel of the Using Agency or the Using Agency's designee to work alongside Contractor Personnel to shadow their role and enable knowledge transfer; answer questions; and explain procedures, tools, utilities, standards and operations used to perform the terminated Services.

9.11. Change Freeze. Unless otherwise approved by the Using Agency or required on an emergency basis to maintain the performance of the Services in accordance with the Performance Standards and SLAs, during the Exit Assistance Period, Contractor will not make or authorize material Changes to: (a) the terminated Services, including to any Equipment, Software or other facilities used to perform the terminated Services; and (b) any contracts entered into by Contractor that relate to the Services (including contracts with Subcontractors).

9.12. Software Licenses. If and as requested by the Using Agency as part of the Exit Assistance Services, Contractor shall: (a) re-assign licenses to the Using Agency or the Using Agency's

designee any licenses for which Contractor obtained Required Consents; (b) grant to the Using Agency, effective as of the Termination Date, at no cost to the Using Agency, a license under Contractor's then-current standard license terms made generally available by Contractor to its other commercial customers in and to all Contractor-Provided Software that constitutes generally commercially available Software that was used by Contractor on a dedicated basis to perform the Services and is reasonably required for the continued operation of the supported environment or to enable the Using Agency to receive services substantially similar to the Services for which Contractor utilized such Software; and with respect to such Software, Contractor shall offer to the Using Agency maintenance (including all enhancements and upgrades) at the lesser of a reasonable rate or the rates Contractor offers to other commercial customers for services of a similar nature and scope; (c) grant to the Using Agency, effective as of the Termination Date, a non-exclusive, non-transferable, fully-paid, royalty-free, perpetual, irrevocable, worldwide license following expiration of the Exit Assistance Period in and to all Contractor-Provided Software that does not constitute generally commercially available Software that is incorporated into the supported environment, which license shall extend only to the use of such Software by the Using Agency or its designee (subject to Contractor's reasonable confidentiality requirements) to continue to enable the Using Agency to receive services substantially similar to the Services for which Contractor utilized such Software; and (d) provide the Using Agency with a copy of the Contractor-Provided Software described in this Section in such media as requested by the Using Agency, together with object code and appropriate documentation.

10. MISCELLANEOUS

10.1. Survival. Sections 1 (Definitions for Special Conditions), 4 (Intellectual Property), 7 (Data Security Breach), and 8 (Audit Rights) shall survive the expiration or termination of this Agreement for a period of five (5) years (and Sections 5 (Using Agency Data and Confidentiality) and 10 (Miscellaneous) shall survive for a period of ten [10] years) from the later of (a) the expiration or termination of this Agreement (including any Exit Assistance Period), or (b) the return or destruction of Using Agency Confidential Information as required by this Agreement.

10.2. No Limitation. The rights and obligations set forth in these IT special conditions exhibit do not limit the rights and obligations set forth in any Articles of the Professional Services Agreement. For the avoidance of doubt, the use of County in the PSA or GC shall expressly include Using Agency and vice versa.

10.3. No Waiver of Tort Immunity. Nothing in this Agreement waives immunity available to the Using Agency under Law, including under the Illinois Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/1-101 et seq.

10.4. No Click-Wrap or Incorporated Terms. The Using Agency is not bound by any content on the Contractor's website, in any click-wrap, shrink-wrap, browse-wrap or other similar document, even if the Contractor's documentation specifically referenced that content and attempts to incorporate it into any other communication, unless the Using Agency has actual knowledge of the content and has expressly agreed to be bound by it in a writing that has been manually signed by the County's Chief Procurement Officer.

10.5. Change Requests. Except as otherwise set forth in this Agreement, this Section 10.5 shall govern all Change Requests and Change Orders. If either Party believes that a Change Order is necessary or desirable, such Party shall submit a Change Request to the other. Contractor represents to Using Agency that it has factored into Contractor's fees adequate contingencies for *de minimis* Change Orders. Accordingly, if Change Requests are made, they will be presumed not to impact the fees under this Agreement; provided, however, that if the Change Request consists of other than a *de minimis* deviation from the scope of the Services and/or Deliverables, Contractor shall provide Using Agency with written notification of such other deviation within five (5) business days after receipt of the Change Request. In the event of a Using Agency-initiated Change Request, within five (5) business days of Contractor's receipt of such Change Request, Contractor shall provide to Using Agency a written statement describing in detail: (a) the reasonably anticipated impact on any Services and Deliverables as a result of the Change Request including, without limitation, Changes in Software and Equipment, and (b) the fixed cost or cost estimate for the Change Request. If Licensor submits a Change Request to Customer, such Change Request shall include the information required for a Change Response.

10.6. Change Orders. Any Change Order that increases the cost or scope of the Agreement, or that materially affects the rights or duties of the Parties as set forth the Agreement, must be agreed upon by the Using Agency in a writing executed by the County's Chief Procurement Officer. In all cases, the approval of all Change Requests and issuance of corresponding Change Orders must comply the County's Procurement Code. If either Party rejects the other's Change Request, Contractor shall proceed to fulfill its obligations under this Agreement.

EXHIBIT 12

Economic Disclosure Statement

**COOK COUNTY
ECONOMIC DISCLOSURE STATEMENT
AND EXECUTION DOCUMENT
INDEX**

Section	Description	Pages
1	Instructions for Completion of EDS	EDS i - ii
2	Certifications	EDS 1- 2
3	Economic and Other Disclosures, Affidavit of Child Support Obligations, Disclosure of Ownership Interest and Familial Relationship Disclosure Form	EDS 3 - 12
4	Cook County Affidavit for Wage Theft Ordinance	EDS 13-14
5	Contract and EDS Execution Page	EDS 15-17
6	Cook County Signature Page	EDS 18

SECTION 1
INSTRUCTIONS FOR COMPLETION OF
ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

This Economic Disclosure Statement and Execution Document ("EDS") is to be completed and executed by every Bidder on a County contract, every Proposer responding to a Request for Proposals, and every Respondent responding to a Request for Qualifications, and others as required by the Chief Procurement Officer. The execution of the EDS shall serve as the execution of a contract awarded by the County. The Chief Procurement Officer reserves the right to request that the Bidder or Proposer, or Respondent provide an updated EDS on an annual basis.

Definitions. Terms used in this EDS and not otherwise defined herein shall have the meanings given to such terms in the Instructions to Bidders, General Conditions, Request for Proposals, Request for Qualifications, as applicable.

Affiliate means a person that directly or indirectly through one or more intermediaries, Controls is Controlled by, or is under common Control with the Person specified.

Applicant means a person who executes this EDS.

Bidder means any person who submits a Bid.

Code means the Code of Ordinances, Cook County, Illinois available on municode.com.

Contract shall include any written document to make Procurements by or on behalf of Cook County.

Contractor or Contracting Party means a person that enters into a Contract with the County.

Control means the unfettered authority to directly or indirectly manage governance, administration, work, and all other aspects of a business.

EDS means this complete Economic Disclosure Statement and Execution Document, including all sections listed in the Index and any attachments.

Joint Venture means an association of two or more Persons proposing to perform a for-profit business enterprise. Joint Ventures must have an agreement in writing specifying the terms and conditions of the relationship between the partners and their relationship and respective responsibility for the Contract

Lobby or lobbying means to, for compensation, attempt to influence a County official or County employee with respect to any County matter.

Lobbyist means any person who lobbies.

Person or Persons means any individual, corporation, partnership, Joint Venture, trust, association, Limited Liability Company, sole proprietorship or other legal entity.

Prohibited Acts means any of the actions or occurrences which form the basis for disqualification under the Code, or under the Certifications hereinafter set forth.

Proposal means a response to an RFP.

Proposer means a person submitting a Proposal.

Response means response to an RFQ.

Respondent means a person responding to an RFQ.

RFP means a Request for Proposals issued pursuant to this Procurement Code.

RFQ means a Request for Qualifications issued to obtain the qualifications of interested parties.

**INSTRUCTIONS FOR COMPLETION OF
ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT**

Section 1: Instructions. Section 1 sets forth the instructions for completing and executing this EDS.

Section 2: Certifications. Section 2 sets forth certifications that are required for contracting parties under the Code and other applicable laws. Execution of this EDS constitutes a warranty that all the statements and certifications contained, and all the facts stated, in the Certifications are true, correct and complete as of the date of execution.

Section 3: Economic and Other Disclosures Statement. Section 3 is the County's required Economic and Other Disclosures Statement form. Execution of this EDS constitutes a warranty that all the information provided in the EDS is true, correct and complete as of the date of execution, and binds the Applicant to the warranties, representations, agreements and acknowledgements contained therein.

Required Updates. The Applicant is required to keep all information provided in this EDS current and accurate. In the event of any change in the information provided, including but not limited to any change which would render inaccurate or incomplete any certification or statement made in this EDS, the Applicant shall supplement this EDS up to the time the County takes action, by filing an amended EDS or such other documentation as is required.

Additional Information. The County's Governmental Ethics and Campaign Financing Ordinances impose certain duties and obligations on persons or entities seeking County contracts, work, business, or transactions, and the Applicant is expected to comply fully with these ordinances. For further information please contact the Director of Ethics at (312) 603-4304 (69 W. Washington St. Suite 3040, Chicago, IL 60602) or visit the web-site at cookcountyl.gov/ethics-board-of.

Authorized Signers of Contract and EDS Execution Page. If the Applicant is a corporation, the President and Secretary must execute the EDS. In the event that this EDS is executed by someone other than the President, attach hereto a certified copy of that section of the Corporate By-Laws or other authorization by the Corporation, satisfactory to the County that permits the person to execute EDS for said corporation. If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a partnership or joint venture, all partners or joint venturers must execute the EDS, unless one partner or joint venture has been authorized to sign for the partnership or joint venture, in which case, the partnership agreement, resolution or evidence of such authority satisfactory to the Office of the Chief Procurement Officer must be submitted with this Signature Page.

If the Applicant is a member-managed LLC all members must execute the EDS, unless otherwise provided in the operating agreement, resolution or other corporate documents. If the Applicant is a manager-managed LLC, the manager(s) must execute the EDS. The Applicant must attach either a certified copy of the operating agreement, resolution or other authorization, satisfactory to the County, demonstrating such person has the authority to execute the EDS on behalf of the LLC. If the LLC is not registered in the State of Illinois, a copy of a current Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.

If the Applicant is a Sole Proprietorship, the sole proprietor must execute the EDS.

A "Partnership" "Joint Venture" or "Sole Proprietorship" operating under an Assumed Name must be registered with the Illinois county in which it is located, as provided in 805 ILCS 405 (2012), and documentation evidencing registration must be submitted with the EDS.

SECTION 2

CERTIFICATIONS

THE FOLLOWING CERTIFICATIONS ARE MADE PURSUANT TO STATE LAW AND THE CODE. THE APPLICANT IS CAUTIONED TO CAREFULLY READ THESE CERTIFICATIONS PRIOR TO SIGNING THE SIGNATURE PAGE. SIGNING THE SIGNATURE PAGE SHALL CONSTITUTE A WARRANTY BY THE APPLICANT THAT ALL THE STATEMENTS, CERTIFICATIONS AND INFORMATION SET FORTH WITHIN THESE CERTIFICATIONS ARE TRUE, COMPLETE AND CORRECT AS OF THE DATE THE SIGNATURE PAGE IS SIGNED. THE APPLICANT IS NOTIFIED THAT IF THE COUNTY LEARNS THAT ANY OF THE FOLLOWING CERTIFICATIONS WERE FALSELY MADE, THAT ANY CONTRACT ENTERED INTO WITH THE APPLICANT SHALL BE SUBJECT TO TERMINATION.

A. PERSONS AND ENTITIES SUBJECT TO DISQUALIFICATION

No person or business entity shall be awarded a contract or sub-contract, for a period of five (5) years from the date of conviction or entry of a plea or admission of guilt, civil or criminal, if that person or business entity:

- 1) Has been convicted of an act committed, within the State of Illinois, of bribery or attempting to bribe an officer or employee of a unit of state, federal or local government or school district in the State of Illinois in that officer's or employee's official capacity;
- 2) Has been convicted by federal, state or local government of an act of bid-rigging or attempting to rig bids as defined in the Sherman Anti-Trust Act and Clayton Act. Act. 15 U.S.C. Section 1 *et seq.*;
- 3) Has been convicted of bid-rigging or attempting to rig bids under the laws of federal, state or local government;
- 4) Has been convicted of an act committed, within the State, of price-fixing or attempting to fix prices as defined by the Sherman Anti-Trust Act and the Clayton Act. 15 U.S.C. Section 1, *et seq.*;
- 5) Has been convicted of price-fixing or attempting to fix prices under the laws the State;
- 6) Has been convicted of defrauding or attempting to defraud any unit of state or local government or school district within the State of Illinois;
- 7) Has made an admission of guilt of such conduct as set forth in subsections (1) through (6) above which admission is a matter of record, whether or not such person or business entity was subject to prosecution for the offense or offenses admitted to; or
- 8) Has entered a plea of *nolo contendere* to charge of bribery, price-fixing, bid-rigging, or fraud, as set forth in subparagraphs (1) through (6) above.

In the case of bribery or attempting to bribe, a business entity may not be awarded a contract if an official, agent or employee of such business entity committed the Prohibited Act on behalf of the business entity and pursuant to the direction or authorization of an officer, director or other responsible official of the business entity, and such Prohibited Act occurred within three years prior to the award of the contract. In addition, a business entity shall be disqualified if an owner, partner or shareholder controlling, directly or indirectly, 20% or more of the business entity, or an officer of the business entity has performed any Prohibited Act within five years prior to the award of the Contract.

THE APPLICANT HEREBY CERTIFIES THAT: The Applicant has read the provisions of Section A, Persons and Entities Subject to Disqualification, that the Applicant has not committed any Prohibited Act set forth in Section A, and that award of the Contract to the Applicant would not violate the provisions of such Section or of the Code.

B. BID-RIGGING OR BID ROTATING

THE APPLICANT HEREBY CERTIFIES THAT: In accordance with 720 ILCS 5/33 E-11, neither the Applicant nor any Affiliated Entity is barred from award of this Contract as a result of a conviction for the violation of State laws prohibiting bid-rigging or bid rotating.

C. DRUG FREE WORKPLACE ACT

THE APPLICANT HEREBY CERTIFIES THAT: The Applicant will provide a drug free workplace, as required by (30 ILCS 580/3).

D. DELINQUENCY IN PAYMENT OF TAXES

THE APPLICANT HEREBY CERTIFIES THAT: *The Applicant is not an owner or a party responsible for the payment of any tax or fee administered by Cook County, by a local municipality, or by the Illinois Department of Revenue, which such tax or fee is delinquent, such as bar award of a contract or subcontract pursuant to the Code, Chapter 34, Section 34-171.*

E. HUMAN RIGHTS ORDINANCE

No person who is a party to a contract with Cook County ("County") shall engage in unlawful discrimination or sexual harassment against any individual in the terms or conditions of employment, credit, public accommodations, housing, or provision of County facilities, services or programs (Code Chapter 42, Section 42-30 *et seq.*).

F. ILLINOIS HUMAN RIGHTS ACT

THE APPLICANT HEREBY CERTIFIES THAT: *It is in compliance with the Illinois Human Rights Act (775 ILCS 5/2-105), and agrees to abide by the requirements of the Act as part of its contractual obligations.*

G. INSPECTOR GENERAL (COOK COUNTY CODE, CHAPTER 34, SECTION 34-174 and Section 34-250)

The Applicant has not willfully failed to cooperate in an investigation by the Cook County Independent Inspector General or to report to the Independent Inspector General any and all information concerning conduct which they know to involve corruption, or other criminal activity, by another county employee or official, which concerns his or her office of employment or County related transaction.

The Applicant has reported directly and without any undue delay any suspected or known fraudulent activity in the County's Procurement process to the Office of the Cook County Inspector General.

H. CAMPAIGN CONTRIBUTIONS (COOK COUNTY CODE, CHAPTER 2, SECTION 2-585)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning campaign contributions, which is codified at Chapter 2, Division 2, Subdivision II, Section 585, and can be read in its entirety at www.municode.com.

I. GIFT BAN, (COOK COUNTY CODE, CHAPTER 2, SECTION 2-574)

THE APPLICANT CERTIFIES THAT: It has read and shall comply with the Cook County's Ordinance concerning receiving and soliciting gifts and favors, which is codified at Chapter 2, Division 2, Subdivision II, Section 574, and can be read in its entirety at www.municode.com.

J. LIVING WAGE ORDINANCE PREFERENCE (COOK COUNTY CODE, CHAPTER 34, SECTION 34-160;

Unless expressly waived by the Cook County Board of Commissioners, the Code requires that a living wage must be paid to individuals employed by a Contractor which has a County Contract and by all subcontractors of such Contractor under a County Contract, throughout the duration of such County Contract. The amount of such living wage is annually by the Chief Financial Officer of the County, and shall be posted on the Chief Procurement Officer's website.

The term "Contract" as used in Section 4, I, of this EDS, specifically excludes contracts with the following:

- 1) Not-For Profit Organizations (defined as a corporation having tax exempt status under Section 501(C)(3) of the United State Internal Revenue Code and recognized under the Illinois State not-for-profit law);
- 2) Community Development Block Grants;
- 3) Cook County Works Department;
- 4) Sheriff's Work Alternative Program; and
- 5) Department of Correction inmates.

SECTION 3

REQUIRED DISCLOSURES

1. DISCLOSURE OF LOBBYIST CONTACTS

List all persons that have made lobbying contacts on your behalf with respect to this contract:

Name

Address

Dell SecureWorks Response: None

2. LOCAL BUSINESS PREFERENCE STATEMENT (CODE, CHAPTER 34, SECTION 34-230)

Local business means a Person, including a foreign corporation authorized to transact business in Illinois, having a bona fide establishment located within the County at which it is transacting business on the date when a Bid is submitted to the County, and which employs the majority of its regular, full-time work force within the County. A Joint Venture shall constitute a Local Business if one or more Persons that qualify as a "Local Business" hold interests totaling over 50 percent in the Joint Venture, even if the Joint Venture does not, at the time of the Bid submittal, have such a bona fide establishment within the County.

a) Is Applicant a "Local Business" as defined above?

Yes: _____ No: X

b) If yes, list business addresses within Cook County:

c) Does Applicant employ the majority of its regular full-time workforce within Cook County?

Yes: _____ No: _____

3. THE CHILD SUPPORT ENFORCEMENT ORDINANCE (CODE, CHAPTER 34, SECTION 34-172)

Every Applicant for a County Privilege shall be in full compliance with any child support order before such Applicant is entitled to receive or renew a County Privilege. When delinquent child support exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

All Applicants are required to review the Cook County Affidavit of Child Support Obligations attached to this EDS (EDS-5) and complete the Affidavit, based on the instructions in the Affidavit.

4. REAL ESTATE OWNERSHIP DISCLOSURES.

The Applicant must indicate by checking the appropriate provision below and providing all required information that either:

- a) The following is a complete list of all real estate owned by the Applicant in Cook County:

PERMANENT INDEX NUMBER(S): _____

(ATTACH SHEET IF NECESSARY TO LIST ADDITIONAL INDEX
NUMBERS)

OR:

- b) ☒ The Applicant owns no real estate in Cook County.

5. EXCEPTIONS TO CERTIFICATIONS OR DISCLOSURES.

If the Applicant is unable to certify to any of the Certifications or any other statements contained in this EDS and not explained elsewhere in this EDS, the Applicant must explain below:

Dell SecureWorks Response: None

If the letters, "NA", the word "None" or "No Response" appears above, or if the space is left blank, it will be conclusively presumed that the Applicant certified to all Certifications and other statements contained in this EDS.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing.

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"Applicant" means any Entity or person making an application to the County for any County Action.

"County Action" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"Person" "Entity" or "Legal Entity" means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and
2. A Person that holds stock or a beneficial interest in the Applicant and is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

This Statement is being made by the ☒ Applicant or ☐ Stock/Beneficial Interest Holder

This Statement is an: ☒ Original Statement or ☐ Amended Statement

Identifying Information:

Name SECUREWORKS, INC.

D/B/A: DELL SECUREWORKS

FEIN NO.: 26-2032356

Street Address: One Concourse Parkway, Suite 500

City: Atlanta

State: GA

Zip Code: 30328

Phone No.: 404-327-6339

Fax Number: 404-728-0144

Email: info@secureworks.com

Cook County Business Registration Number: _____

(Sole Proprietor, Joint Venture Partnership)

Corporate File Number (if applicable): _____

Form of Legal Entity:

☐ Sole Proprietor ☐ Partnership ☐ Corporation ☐ Trustee of Land Trust

☐ Business Trust ☐ Estate ☐ Association ☐ Joint Venture

☒ Other (describe) WHOLLY OWNED SUBSIDIARY OF DELL INC.

Ownership Interest Declaration:

List the name(s), address, and percent ownership of each Person having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder
------	---------	---

Dell SecureWorks Response: None

2. If the interest of any Person listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address
-----------------------	-------------------	---------------------

Not applicable

3. Is the Applicant constructively controlled by another person or Legal Entity? ☒ Yes ☐ No

If yes, state the name, address and percentage of beneficial interest of such person, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship
DELL INC.	One Dell Way, Round Rock, TX 78682	100 %	Parent Company

Corporate Officers, Members and Partners Information:

For all corporations, list the names, addresses, and terms for all corporate officers. For all limited liability companies, list the names, addresses for all members. For all partnerships and joint ventures, list the names, addresses, for each partner or joint venture.

Name	Address	Title (specify title of Office, or whether manager or partner/joint venture)	Term of Office
<u>Michael Dell</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>Chief Executive Officer</u>	<u>since 1984</u>
<u>Marius Haas</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>Chief Commercial Officer and President</u>	
<u>Karen Quintos</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>Chief Marketing Officer</u>	
<u>Richard Rothberg,</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>SVP, General Counsel</u>	
<u>Thomas Sweet</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>SVP, Chief Financial Officer</u>	
<u>Jeffrey Clarke</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>Vice Chairman, Operations and President, Client Solutions</u>	
<u>Steve Price,</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>SVP, Human Resources</u>	
<u>Rory Read</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>Chief Integration Officer</u>	
<u>John Swainson,</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>President, Software</u>	
<u>Sures Vaswani,</u>	<u>One Dell Way, Round Rock, TX 78682</u>	<u>President, Services</u>	

Declaration (check the applicable box):

- ☒ I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor reserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.
- ☐ I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT SIGNATURE PAGE

SecureWorks, Inc.
Name of Authorized Applicant/Holder Representative (please print or type)
David F. Baum
Signature
dbaum@secureworks.com
E-mail address

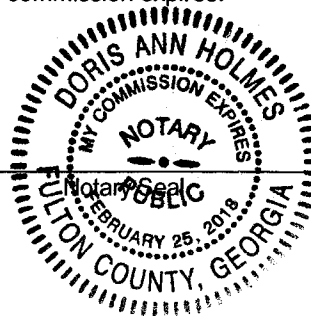
Legal Director
Title
11/23/15
Date
404-235-0195
Phone Number

Subscribed to and sworn before me

this 23 day of Nov, 2015.

X [Signature]
Notary Public Signature

My commission expires:





COOK COUNTY BOARD OF ETHICS
 69 W. WASHINGTON STREET, SUITE 3040
 CHICAGO, ILLINOIS 60602
 312/603-4304 Office 312/603-9988 Fax

FAMILIAL RELATIONSHIP DISCLOSURE PROVISION

Nepotism Disclosure Requirement:

Doing a significant amount of business with the County requires that you disclose to the Board of Ethics the existence of any familial relationships with any County employee or any person holding elective office in the State of Illinois, the County, or in any municipality within the County. The Ethics Ordinance defines a significant amount of business for the purpose of this disclosure requirement as more than \$25,000 in aggregate County leases, contracts, purchases or sales in any calendar year.

If you are unsure of whether the business you do with the County or a County agency will cross this threshold, err on the side of caution by completing the attached familial disclosure form because, among other potential penalties, any person found guilty of failing to make a required disclosure or knowingly filing a false, misleading, or incomplete disclosure will be prohibited from doing any business with the County for a period of three years. The required disclosure should be filed with the Board of Ethics by January 1 of each calendar year in which you are doing business with the County and again with each bid/proposal/quotation to do business with Cook County. The Board of Ethics may assess a late filing fee of \$100 per day after an initial 30-day grace period.

The person that is doing business with the County must disclose his or her familial relationships. If the person on the County lease or contract or purchasing from or selling to the County is a business entity, then the business entity must disclose the familial relationships of the individuals who are and, during the year prior to doing business with the County, were:

- its board of directors,
- its officers,
- its employees or independent contractors responsible for the general administration of the entity,
- its agents authorized to execute documents on behalf of the entity, and
- its employees who directly engage or engaged in doing work with the County on behalf of the entity.

Do not hesitate to contact the Board of Ethics at (312) 603-4304 for assistance in determining the scope of any required familial relationship disclosure.

Additional Definitions:

"Familial relationship" means a person who is a spouse, domestic partner or civil union partner of a County employee or State, County or municipal official, or any person who is related to such an employee or official, whether by blood, marriage or adoption, as a:

- | | | |
|----------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Parent | <input type="checkbox"/> Grandparent | <input type="checkbox"/> Stepfather |
| <input type="checkbox"/> Child | <input type="checkbox"/> Grandchild | <input type="checkbox"/> Stepmother |
| <input type="checkbox"/> Brother | <input type="checkbox"/> Father-in-law | <input type="checkbox"/> Stepson |
| <input type="checkbox"/> Sister | <input type="checkbox"/> Mother-in-law | <input type="checkbox"/> Stepdaughter |
| <input type="checkbox"/> Aunt | <input type="checkbox"/> Son-in-law | <input type="checkbox"/> Stepbrother |
| <input type="checkbox"/> Uncle | <input type="checkbox"/> Daughter-in-law | <input type="checkbox"/> Stepsister |
| <input type="checkbox"/> Niece | <input type="checkbox"/> Brother-in-law | <input type="checkbox"/> Half-brother |
| <input type="checkbox"/> Nephew | <input type="checkbox"/> Sister-in-law | <input type="checkbox"/> Half-sister |

**COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM**

A. PERSON DOING OR SEEKING TO DO BUSINESS WITH THE COUNTY

Name of Person Doing Business with the County: Entity = Dell SecureWorks

Address of Person Doing Business with the County: One Concourse Parkway Suite 500, Atlanta, GA 30328

Phone number of Person Doing Business with the County: David Baum, 404-327-6339

Email address of Person Doing Business with the County: Legal@secureworks.com

If Person Doing Business with the County is a Business Entity, provide the name, title and contact information for the individual completing this disclosure on behalf of the Person Doing Business with the County:

David Baum, Senior Legal Counsel, 404-327-6339, legal@secureworks.com

B. DESCRIPTION OF BUSINESS WITH THE COUNTY

Append additional pages as needed and for each County lease, contract, purchase or sale sought and/or obtained during the calendar year of this disclosure (or the proceeding calendar year if disclosure is made on January 1), identify:

The lease number, contract number, purchase order number, request for proposal number and/or request for qualification number associated with the business you are doing or seeking to do with the County: _____

RFP No. 1550-14939

The aggregate dollar value of the business you are doing or seeking to do with the County: \$ _____

The name, title and contact information for the County official(s) or employee(s) involved in negotiating the business you are doing or seeking to do with the County: _____

The name, title and contact information for the County official(s) or employee(s) involved in managing the business you are doing or seeking to do with the County: _____

C. DISCLOSURE OF FAMILIAL RELATIONSHIPS WITH COUNTY EMPLOYEES OR STATE, COUNTY OR MUNICIPAL ELECTED OFFICIALS

Check the box that applies and provide related information where needed

☐ The Person Doing Business with the County is **an individual** and there is **no familial relationship** between this individual and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

DB
X
11/23/15
☒ The Person Doing Business with the County is **a business entity** and there is **no familial relationship** between any member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity or employees directly engaged in contractual work with the County on behalf of the business entity, and any Cook County employee or any person holding elective office in the State of Illinois, Cook County, or any municipality within Cook County.

**COOK COUNTY BOARD OF ETHICS
FAMILIAL RELATIONSHIP DISCLOSURE FORM**

- ☐ The Person Doing Business with the County is an individual and there is a familial relationship between this individual and at least one Cook County employee and/or a person or persons holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County. **The familial relationships are as follows:**

Name of Individual Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

If more space is needed, attach an additional sheet following the above format.

- ☐ The Person Doing Business with the County is a business entity and there is a familial relationship between at least one member of this business entity's board of directors, officers, persons responsible for general administration of the business entity, agents authorized to execute documents on behalf of the business entity and/or employees directly engaged in contractual work with the County on behalf of the business entity, on the one hand, and at least one Cook County employee and/or a person holding elective office in the State of Illinois, Cook County, and/or any municipality within Cook County, on the other. **The familial relationships are as follows:**

Name of Member of Board of Director for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Name of Officer for Business Entity Doing Business with the County	Name of Related County Employee or State, County or Municipal Elected Official	Title and Position of Related County Employee or State, County or Municipal Elected Official	Nature of Familial Relationship*
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Name of Person Responsible
for the General
Administration of the
Business Entity Doing
Business with the County

Name of Related County
Employee or State, County or
Municipal Elected Official

Title and Position of Related
County Employee or State, County
or Municipal Elected Official

Nature of Familial
Relationship*

Name of Agent Authorized
to Execute Documents for
Business Entity Doing
Business with the County

Name of Related County
Employee or State, County or
Municipal Elected Official

Title and Position of Related
County Employee or State, County
or Municipal Elected Official

Nature of Familial
Relationship*

Name of Employee of
Business Entity Directly
Engaged in Doing Business
with the County

Name of Related County
Employee or State, County or
Municipal Elected Official

Title and Position of Related
County Employee or State, County
or Municipal Elected Official

Nature of Familial
Relationship*

If more space is needed, attach an additional sheet following the above format.

VERIFICATION: To the best of my knowledge, the information I have provided on this disclosure form is accurate and complete. I acknowledge that an inaccurate or incomplete disclosure is punishable by law, including but not limited to fines and debarment.

David T. Baum
Signature of Recipient

11/23/15
Date

SUBMIT COMPLETED FORM TO:

Cook County Board of Ethics
69 West Washington Street, Suite 3040, Chicago, Illinois 60602
Office (312) 603-4304 – Fax (312) 603-9988
CookCounty.Ethics@cookcountyil.gov

* Spouse, domestic partner, civil union partner or parent, child, sibling, aunt, uncle, niece, nephew, grandparent or grandchild by blood, marriage (i.e. in laws and step relations) or adoption.

SECTION 4

COOK COUNTY AFFIDAVIT FOR WAGE THEFT ORDINANCE

Effective May 1, 2015, every Person, **including Substantial Owners**, seeking a Contract with Cook County must comply with the Cook County Wage Theft Ordinance set forth in Chapter 34, Article IV, Section 179. Any Person/Substantial Owner, who fails to comply with Cook County Wage Theft Ordinance, may request that the Chief Procurement Officer grant a reduction or waiver in accordance with Section 34-179(d).

"Contract" means any written document to make Procurements by or on behalf of Cook County.

"Person" means any individual, corporation, partnership, Joint Venture, trust, association, limited liability company, sole proprietorship or other legal entity.

"Procurement" means obtaining supplies, equipment, goods, or services of any kind.

"Substantial Owner" means any person or persons who own or hold a twenty-five percent (25%) or more percentage of interest in any business entity seeking a County Privilege, including those shareholders, general or limited partners, beneficiaries and principals; except where a business entity is an individual or sole proprietorship, Substantial Owner means that individual or sole proprietor.

All Persons/Substantial Owners are required to complete this affidavit and comply with the Cook County Wage Theft Ordinance before any Contract is awarded. Signature of this form constitutes a certification the information provided below is correct and complete, and that the individual(s) signing this form has/have personal knowledge of such information.

I. Contract Information:

Contract Number: RFP No. 1550-14939

County Using Agency (requesting Procurement): Cook County, Illinois

II. Person/Substantial Owner Information:

Person (Corporate Entity Name): SecureWorks Inc. doing business as Dell SecureWorks

Substantial Owner Complete Name: Michael Dell

EIN# 26-2032356

Date of Birth: confidential

E-mail address: legal@secureworks.com

Street Address: One Dell Way

City: Round Rock

State: TX Zip: 78682

Home Phone: () confidential

Driver's License No: confidential

III. Compliance with Wage Laws:

Within the past five years has the Person/Substantial Owner, in any judicial or administrative proceeding, been convicted of, entered a plea, made an admission of guilt or liability, or had an administrative finding made for committing a repeated or willful violation of any of the following laws:

Illinois Wage Payment and Collection Act, 820 ILCS 115/1 et seq., **NO**

Illinois Minimum Wage Act, 820 ILCS 105/1 et seq., **NO**

Illinois Worker Adjustment and Retraining Notification Act, 820 ILCS 65/1 et seq., **NO**

Employee Classification Act, 820 ILCS 185/1 et seq., **NO**

Fair Labor Standards Act of 1938, 29 U.S.C. 201, et seq., **NO**

Any comparable state statute or regulation of any state, which governs the payment of wages **NO**

If the Person/Substantial Owner answered "Yes" to any of the questions above, it is ineligible to enter into a Contract with Cook County, but can request a reduction or waiver under **Section IV**.

IV. Request for Waiver or Reduction

If Person/Substantial Owner answered "Yes" to any of the questions above, it may request a reduction or waiver in accordance with Section 34-179(d), provided that the request for reduction of waiver is made on the basis of one or more of the following actions that have taken place:

There has been a bona fide change in ownership or Control of the ineligible Person or Substantial Owner
YES or NO

Disciplinary action has been taken against the individual(s) responsible for the acts giving rise to the violation
YES or NO

Remedial action has been taken to prevent a recurrence of the acts giving rise to the disqualification or default
YES or NO

Other factors that the Person or Substantial Owner believe are relevant.
YES or NO

The Person/Substantial Owner must submit documentation to support the basis of its request for a reduction or waiver. The Chief Procurement Officer reserves the right to make additional inquiries and request additional documentation.

V. Affirmation

The Person/Substantial Owner affirms that all statements contained in the Affidavit are true, accurate and complete.

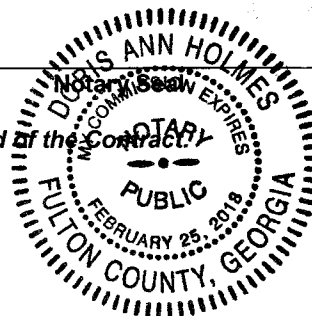
Signature: David P. Baum Date: 11/23/15

Name of Person signing (Print): David P. Baum Title: Legal Director

Subscribed and sworn to before me this 24 day of November, 2015

X [Signature]
 Notary Public Signature

Note: The above information is subject to verification prior to the award of the Contract.



SECTION 5

CONTRACT AND EDS EXECUTION PAGE
PLEASE EXECUTE THREE ORIGINAL COPIES

The Applicant hereby certifies and warrants that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Applicant is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Applicant with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Applicant in this EDS are true, complete and correct. The Applicant agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

Execution by Corporation

SecureWorks Inc.

Corporation's Name

Cheryl Shaeck

President's Printed Name and Signature

Cshaeck@secureworks.com

Email

Telephone

None exists

Secretary Signature

Date

7/22/2016

Execution by LLC

LLC Name

*Member/Manager Printed Name and Signature

Date

Telephone and Email

Execution by Partnership/Joint Venture

Partnership/Joint Venture Name

*Partner/Joint Venturer Printed Name and Signature

Date

Telephone and Email

Execution by Sole Proprietorship

Printed Name and Signature

Date

Telephone

Email

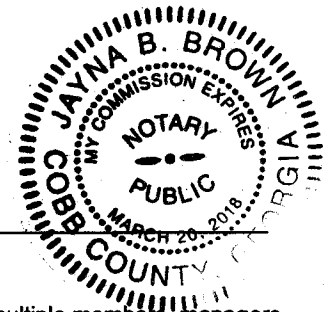
Subscribed and sworn to before me this
22nd day of July, 2016.

Jayna B. Brown
 Notary Public Signature

My commission expires:

3/20/2018

Notary Seal



If the operating agreement, partnership agreement or governing documents requiring execution by multiple members, managers, partners, or joint venturers, please complete and execute additional Contract and EDS Execution Pages.

CERTIFICATE OF INCUMBENCY

I, George Hanna, Vice President and General Counsel of SecureWorks, Inc. (the "Firm"), a company duly organized and validly existing under the laws of the state of Georgia, hereby certify as follows:

I have reviewed the constitutional documents and resolutions of the Board of Directors of SecureWorks Corp., a Delaware corporation, of which the Firm is a wholly-owned subsidiary, and certify that the individual named below is authorized to act on behalf of the Firm to sign, execute and deliver, on behalf of the Firm, the Economic Disclosure Statement and Identification of Subcontractor/Supplier/Sub-consultant Form with The County of Cook located in Chicago, IL. The person named below is duly qualified and acting representative of the Firm, duly appointed and authorized to sign the Economic Disclosure Statement and the Identification of Subcontractor/Supplier/Sub-consultant Form aforementioned and all documentation required by The County of Cook located in Chicago, IL for this purpose. The signature set opposite the name of that person is the genuine signature of said person.

Name

Cheryl Strack

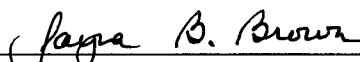
Signature



George Hanna, Vice President and General Counsel of
SecureWorks, Inc.

State of Georgia
County of Cobb

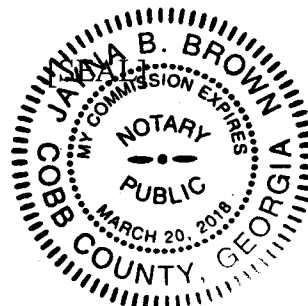
Signed and sworn to before me on this 22nd day of July, 2016, by George Hanna, Vice President and General Counsel of SecureWorks, Inc., a company duly organized and validly existing under the laws of the state of Georgia, who is personally known and/or proved to me on the basis of satisfactory evidence, to be the person who appeared before me.



Notary Public

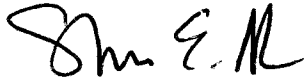
My Commission Expires:

3/20/2018



SECTION 6
COOK COUNTY SIGNATURE PAGE

ON BEHALF OF THE COUNTY OF COOK, A BODY POLITIC AND CORPORATE OF THE STATE OF ILLINOIS, THIS CONTRACT IS HEREBY EXECUTED BY:



COOK COUNTY CHIEF PROCUREMENT OFFICER

DATED AT CHICAGO, ILLINOIS THIS 27 DAY OF July, 2016

IN THE CASE OF A BID/ PROPOSAL/RESPONSE, THE COUNTY HEREBY ACCEPTS:

THE FOREGOING BID/PROPOSAL/RESPONSE AS IDENTIFIED IN THE CONTRACT DOCUMENTS FOR CONTRACT NUMBER
1550-14939OR

ITEM(S), SECTION(S), PART(S): _____

TOTAL AMOUNT OF CONTRACT: \$ 2,459,632.50

(DOLLARS AND CENTS)

FUND CHARGEABLE: _____

APPROVED AS TO FORM:



ASSISTANT STATE'S ATTORNEY
(Required on contracts over \$1,000,000.00)7/12/16
DateAPPROVED BY THE BOARD OF
COOK COUNTY COMMISSIONERS

JUL 13 2016